ChipDoc v4.2 on JCOP 4.5 P71 in ICAO BAC configuration

Security Target Lite

Rev. 1.1 — 14 May 2026
Release

Evaluation documentation
PUBLIC

Document information

Info	Content
Keywords	Common Criteria, Security Target, ChipDoc v4.2, JCOP 4.5 P71, ICAO BAC
Abstract	Security Target of ChipDoc v4.2 application on JCOP 4.5 P71 in ICAO BAC configuration, which is developed and provided by NXP Semiconductors. The TOE complies with Evaluation Assurance Level 4 of the Common Criteria for Information Technology Security Evaluation Version 2022 with Augmentations..

Revision history

Rev	Date	Description
1.0	04 May 2026	Created from Security Target
1.1	14 May 2026	Public Version of ST v1.4

1. ST Introduction (ASE_INT)

1.1 ST Reference and TOE Reference

Table 1. ST Reference and TOE Reference

ST Title	ChipDoc v4.2 on JCOP 4.5 P71 in ICAO BAC configuration Security Target
ST Reference	CDv4.2_210311_ST_ICAO_BAC
ST Version	Rev. 1.1
ST Date	14 May 2026
Product Type	Java Card Applet
TOE Name	ChipDoc v4.2 on JCOP 4.5 P71 in ICAO BAC configuration
CC Version	Common Criteria for Information Technology Security Evaluation Version 2022, Revision 1, November 2022

1.2 TOE Overview

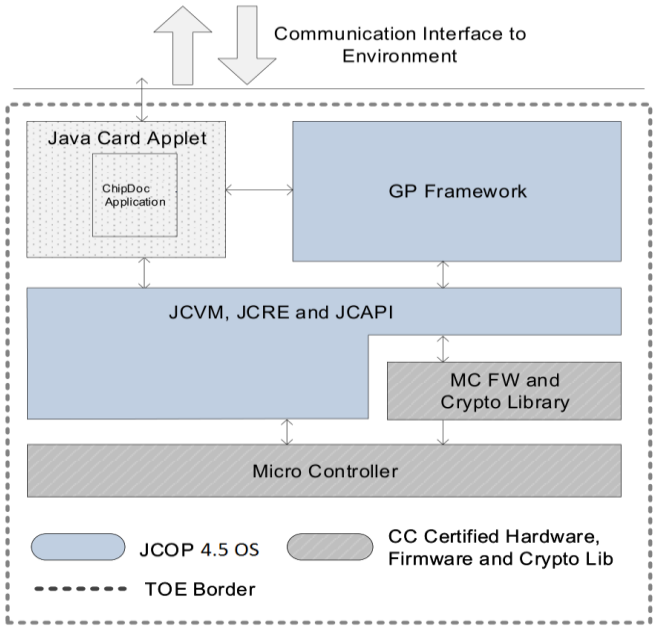

Fig 1. Components of the TOE

The TOE consists of an applet which is executed by a software stack that is stored on a Micro Controller. For a complete picture of the TOE see Fig 1, and for details with regards to the different components see section 1.3.5.

The protection profile [7] defines the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). This ST extends this PP to contact, contactless and dual interface smartcard modules. It addresses the advanced security methods Basic Access Control (BAC) and Active Authentication (AA) according to 'ICAO Doc 9303' [9] using the applicable formulations from the PP-0056 [8] .

ChipDoc v4.2 passport application is configurable in BAC, EAC with BAC or EAC with PACE, with or without Active Authentication. Also, it supports contact and contactless communication.

This ST applies to the BAC configuration with or without Active Authentication.

Note that there is no non-TOE hardware/software/firmware that is required by the TOE.

1.2.1 TOE usage and security features for operational use

The ChipDoc v4.2 application offers variety of applications like electronic identification (eID), electronic driver's license (eDL) or electronic passport (ePP), subject of the current TOE.

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this TOE contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the traveler is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) optional biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the Document Number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [9]. These security measures include the binding of the MRTD's chip to the passport book.

The logical MRTD is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organization and the security features of the MRTD's chip.

The ICAO defines the baseline security methods (Passive Authentication) and the optional advanced security methods (BAC to the logical MRTD, Active Authentication of the MRTD's chip, EAC and PACE to the logical MRTD and the Data Encryption of additional sensitive biometrics) as optional security measure in the 'ICAO Doc 9303' [9]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

This TOE addresses the protection of the logical MRTD (i) in integrity by write only- once access control and by physical means, and (ii) in confidentiality by the BAC Mechanism. This TOE addresses the AA as an optional security mechanism.

1.3 TOE Description

1.3.1 General

The TOE is an MRTD IC where application software is loaded to FLASH, and the TOE can be assembled in a variety of form factors. The main form factor is the electronic passport, a paper book passport embedding a contactless module.

The followings are an informal and non-exhaustive list of example graphic representations of possible end products embedding the TOE:

- Contactless interface cards and modules
- Dual interface cards and modules
- Contact only cards and modules

The scope of this TOE is covered in section 1.2 above and detailed hereafter.

The TOE is linked to a MRTD reader via its HW and physical interfaces.

- The contactless type interface of the TOE smartcard is ISO/IEC 14443 compliant.
- The optional contact type interface of the TOE smartcard is ISO/IEC 7816 compliant.
- The optional interfaces of the TOE SOIC-8 are ISO 9141 compliant.
- The optional interfaces of the TOE QNF-44 are JEDEC compliant.

There are no other external interfaces of the TOE except the ones described above.

The antenna and the packaging, including their external interfaces, are out of the scope of this TOE.

The TOE may be applied to a contact reader or to a contactless reader, depending on the external interface type(s) available in its form factor. The readers are connected to a computer and allow application programs (APs) to use the TOE.

The TOE can embed other secure functionalities, but they are not in the scope of this TOE and subject to an evaluation in other TOEs.

1.3.2 MRTD's chip

For this TOE the MRTD is viewed as unit of

1. The **physical MRTD** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder
   a. the biographical data on the biographical data page of the passport book,

b. the printed data in the Machine Readable Zone (MRZ) and

c. the printed portrait.

2. The **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [9] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder

   a. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),

   b. the digitized portraits (EF.DG2),

   c. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both,

   d. the other data according to LDS (EF.DG5 to EF.DG16) and

   e. the Document security object.

This TOE addresses the protection of the logical MRTD:

- in integrity by write-only-once access control and by physical means, and
- in confidentiality by Basic Access Control Mechanism.

This TOE addresses the Active Authentication stated in [9].

1.3.3 Basic Access Control

The confidentiality by Basic Access Control (BAC) is a mandatory security feature that is implemented by the TOE. For BAC, the inspection system

(i) reads optically the MRTD,
(ii) authenticates itself as an inspection system by means of Document Basic Access Keys.

After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [9], normative appendix 5.

1.3.4 Active Authentication

This TOE offers an optional mechanism called Active Authentication and specified in [10] section 2.4. This security feature is a digital security feature that prevents cloning by introducing a chip-individual key pair:

(i) The public key is stored in data group DG15 and thus protected by Passive Authentication.

(ii) The corresponding private key is stored in secure memory and may only be used internally by the MRTD chip and cannot be read out.

Thus, the chip can prove knowledge of this private key in a challenge-response protocol, which is called Active Authentication. In this protocol the MRTD chip digitally signs a challenge randomly chosen by the inspection system. The inspection system recognizes that the MRTD chip is genuine if and only if the returned signature is correct. Active Authentication is a straightforward protocol and prevents cloning very effectively but introduces a privacy threat: Challenge Semantics (see Appendix F for a discussion on Challenge Semantics).

1.3.5 TOE Components and Composite Certification

The certification of this TOE is a composite certification. This means that for the certification of this TOE other certifications of components which are part of this TOE are re-used. In the following sections more detailed descriptions of the components of Figure 1 are provided. In the description it is also made clear whether a component is covered by a previous certification or whether it is covered in the certification of this TOE.

1.3.5.1 Micro Controller

The Micro Controller is a secure smart card controller from NXP's SmartMX3 family. The Micro Controller contains a co-processor for symmetric cryptographic operations, supporting DES and AES, as well as an accelerator for asymmetric cryptographic algorithms. The Micro Controller further contains a physical random number generator. The supported memory technologies are volatile (Random Access Memory (RAM)) and non-volatile (Read Only Memory (ROM) and FLASH) memory.

Access to all memory types is controlled by a Memory Management Unit (MMU) which allows to separate and restrict access to parts of the memory.

The Micro Controller has been certified in a previous certification and the results are re-used for this certification. The exact reference to the previous certification is given in the following table:

Table 2. Reference to Certified Micro Controller with IC Dedicated Software and Crypto Library

Name	NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3)
Certification ID	BSI-DSZ-CC-1149-V4-2025
Assurance Level	EAL 6 augmented with ALC_FLR.1 and ASE_TSS.1
Reference	[16]

1.3.5.2 Security IC Dedicated Software

Micro Controller Firmware

The Micro Controller Firmware is used for testing of the Micro Controller at production, for booting of the Micro Controller after power-up or after reset, for configuration of communication devices and for writing data to volatile and non-volatile memory.

The Micro Controller Firmware has been certified together with the Micro Controller (refer to Table 2) and the same references ([16]) as given for the Micro Controller also apply for the Micro Controller Firmware.

Crypto Library

The Crypto Library provides implementations for symmetric and asymmetric cryptographic operations, hashing, the generation of hybrid deterministic and hybrid physical random numbers and further tools like secure copy and compare. The symmetric cryptographic operations comprise the algorithms 3DES, AES and KoreanSEED, where these algorithms use the symmetric co-processor of the Micro Controller. The supported asymmetric cryptographic operations are ECC and RSA. These algorithms use the Public Key Crypto Coprocessor (PKCC) of the Micro Controller for the cryptographic operations.

The Crypto Library has been certified together with the Micro Controller (refer to Table 2) and the same references ([16]) as given for the Micro Controller also apply.

1.3.5.3 Security IC Embedded Software

JCOP 4.5 P71

The Operating System consists of JCVM, JCRE, JCAPI and GP framework. It is implemented according to the Java Card Specification and GlobalPlatform and has been certified in the course of a previous certification, where the results are re-used for this certification. The exact reference to the certification is given in the following table:

Table 3. Reference to certified Platform

Name	JCOP 4.5 P71
Certification ID	NSCIB-2300127-02
Assurance Level	EAL6 augmented with ALC_FLR.1 & ASE_TSS.2
Reference	[17]

ChipDoc v4.2 application:

The applet as part of the TOE, programs the underlying integrated circuit chip of machine readable travel documents (MRTD's chip) according to the Logical Data Structure (LDS) [9] and providing the BAC mechanism according to the 'ICAO Doc 9303' [9].

The TOE comprises at least:

- the circuitry of the MRTD's chip (N7122 IC)
- the IC Embedded Software (JCOP 4.5 P71 Operating System)
- the MRTD application (ChipDoc v4.2 applet in ICAO configuration)
- the associated guidance documentation

1.3.6 TOE Lifecycle

The TOE lifecycle is shown in Fig 2 TOE LifeCycle and is described in terms of the four life cycle phases (subdivided to 7 steps) mentioned in PP-0055 [7], but with a refinement in pre-personalisation, to support platform patching by the MRTD manufacturer who operates from a CC certified site.

The IC Developer, IC Manufacturer as well as the MRTD Embedded Software Developer of this TOE is NXP Semiconductors. In particular the software development for this composite TOE mainly took place in "NXP Gratkorn, Mikron-Weg 1, A-8101 Gratkorn, Austria" and "NXP Hamburg, Troplowitzstr. 20, 22529 Hamburg, Germany" and "NXP Glasgow, Pegasus House, Scottish Enterprise Technology Park, Bramah Ave, East Kilbride Glasgow, G75, Scotland United Kindom. All other sites contributing to the Lifecycle of this TOE can be read from the ALC_LCD evidence.

1.3.6.1 Phase 1 "Development"

(Step 1 – IC Design)

The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

(Step 2 – Embedded Software Design)

The embedded software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the operating system, the MRTD application and the guidance documentation associated with these TOE components.

1.3.6.2 Phase 2 “Manufacturing”

(Step 3 – IC Manufacturing)

In the first instance the TOE integrated circuit is produced containing the MRTD’s chip Dedicated Software and the parts of the MRTD’s chip Embedded Software in the non-volatile non-programmable memories (ROM). Other parts of the Embedded Software are loaded into Flash. The IC manufacturer programs IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.

(Step 4 – IC Initialisation)

The Embedded Software which constitutes the Operating System and the Card Content Manager is enabled with the requisite keys loaded and transport mechanisms enabled, which supports the secure transport of the IC from NXP manufacturing facility to the MRTD Manufacturer facility.

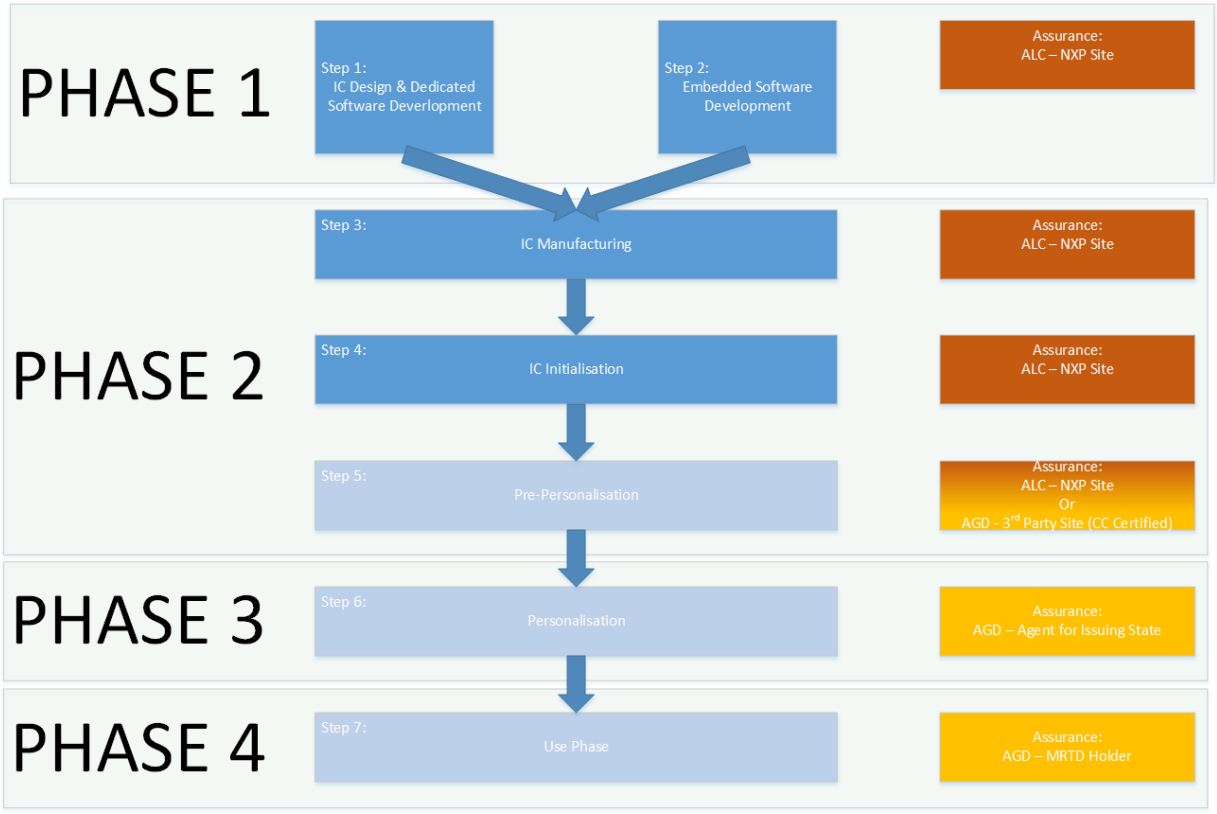

Fig 2. TOE LifeCycle

(Step 5 - PrePersonalisation)

During the step Pre-Perso, the MRTD manufacturer

(i) creates the MRTD application and
(ii) equips MRTD's chips with pre-personalization Data.

IC Pre-Personalization

To create the application, it is necessary to instantiate the applet and create an MRTD file system. In addition to the certified MRTD file system, one or more additional file systems may be present on the TOE. This allows the TOE user to switch between more than one (potentially certified) file systems or configurations of the application. Since the ChipDoc v3.1 application offers electronic identity, driving license or SSCD functionalities in addition to MRTD, the associated file systems may coexist on the TOE.

Any platform patching required is completed at this point. For e-passport products, Card Content Management is finalized in this phase, thus post issuance applet loading is disabled and the platform closed to further amendments.

The pre-personalized MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent. NXP or the MRTD Manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

(Packaging)

The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book.

IC Packaging

MRTD Manufacturing

This step corresponds to the integration of the hardware and firmware components into the final product body. The TOE is protected during transfer between various parties. IC Packaging and MRTD Manufacturing are not part of the scope of this TOE.

1.3.6.3 Phase 3 “Personalization of the MRTD”

(Step 6 - Personalization)

The personalization of the MRTD includes:

- the survey of the MRTD holder’s biographical data,
- the enrolment of the MRTD holder biometric reference data,
- the printing of the visual readable data onto the physical MRTD,
- the writing of the TOE User Data and TSF Data into the logical MRTD and
- configuration of the TSF if necessary.

Step 6 is performed by the Personalization Agent and includes but is not limited to the creation of the digital MRZ data (EF.DG1), the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both, the other data according to LDS (EF.DG5 to EF.DG16) and the Document security object. The signing of the Document security object by the Document signer [9] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Personalization – 3rd Party Personalization facility

The TOE is protected during transfer between various parties by the confidential information which resides in the card during mask production.

In case the personalization is done by 3rd party personalization facility, the Personalization phase is not part of the scope of this TOE.

1.3.6.4 Phase 4 “Operational Use”

Where upon the card is delivered to the MRTD holder and until MRTD is expired or destroyed.

(Step 7)

The TOE is used as MRTD chip by the traveler and the inspection systems in the “Operational Use” phase. The user data can be read according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State but they can never be modified.

The Operational Use phase is not part of the scope of this TOE.

1.3.7 TOE Identification

1.3.7.1 TOE Delivery

The TOE delivery can occur at the end of Step4 when the Pre-personalization is handled by the Provisioning Service Provider, at the end of Step5 when the Pre-personalization is handled by NXP Semiconductors, or at the end of Step2 for field upgrade (see chapter 1.3.6). The delivery comprises the following items:

Table 4. Delivery Items

Type	Name	Version	From of delivery
JCOP 4.5 P71 Platform	NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library ROM Code (Platform ID) FLASH content (FLASH ID) Patch Code (Patch ID)	JCOP 4.5 P71	Micro Controller including on-chip software: Firmware, Crypto Library and JCOP 4.5 Operating System
ChipDoc v4.2 application	FLASH content	4.2.0.52	Application software loaded onto the IC OR Standalone CAP file encrypted and signed according to GP Amd-I [20]
Document	ChipDoc 4.2 Applet User Guide Manual	[18]	Electronic Document encrypted and signed
Document	ChipDoc 4.2 ICAO Personalization Guide	[19]	Electronic Document encrypted and signed
Document	ChipDoc 4.2 Applet Release Note – Release Note for ChipDoc 4.2.0.4JxR Applet	[22]	Electronic Document encrypted and signed

1.3.7.2 Identification of the TOE

The TOE can be identified by

- identifying the JCOP 4.5 P71 platform: The GET_DATA(IDENTIFY) command shall be sent to the TOE to verify the correct values of Platform ID, the ROM ID and the Patch ID as stated in section "2.1 Platform identification" of the ICAO Personalization Guidance for this TOE [19].
- identifying the ICAO application: The ChipDoc v4.2 application and the specific TOE configuration (ICAO BAC) can be verified according the respective instructions in sections “2.2 Applet identification” and “2.3 Applet configuration” of the ICAO Personalization Guidance for this TOE [19].

1.3.8 Evaluated Package Types

A number of package types are supported for this TOE. All package types, which are covered by the certification of the used platform (see [16]), are also allowed to be used in combination with each product of this TOE.

The package types do not influence the security functionality of the TOE. They only define which pads are connected in the package and for what purpose and in which environment the chip can be used. Note that the security of the TOE is not dependent on which pad is connected or not - the connections just define how the product can be used. If the TOE is delivered as wafer the customer can choose the connection on his own.

2. Conformance Claims (ASE_CCL)

2.1 CC Conformance Claim

This Security Target claims to be conformant to the Common Criteria for Information Technology Security Evaluation Version 2022, Revision 1, Nov 2022

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 2022, Revision 1, Nov 2022. CCMB-2022-011-001 [1]
Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 2022, Revision 1, Nov 2022. CCMB-2022-011-002 [2]
Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components Version 2022, Revision 1, Nov 2022. CCMB-2022-011-003 [3]
Common Criteria for Information Technology Security Evaluation, Part 4: Framework fpr the specification of evaluation methods and activities, Version 2022, Revision 1, Nov 2022. CCMB-2022-011-004 [4]
Common Criteria for Information Technology Security Evaluation, Part 5: Pre-Defined packages of security requirements, Version 2022, Revision 1, Nov 2022. CCMB-2022-011-005 [5]

The following methodology will be used for the evaluation:

Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2022, Revision 1, Nov 2022. CCMB-2022-011-006 [6]

This Security Target claims to be CC Part 2 extended and CC Part 3 conformant. The Protection Profile defines extended Security Functional Requirements which are detailed in section 5.

The Extensions are based on the Protection Profiles (PP-0055 [7] and PP-0056 [8]) however are replaced with the CC:2022 equivalents in accordance with the CC:2022 Transition Policy document [24].

In accordance with the CC:2022 Transition Policy document [24], instances of FCS_CKM.4 are replaced by the definition of FCS_CKM.6 found in CC:2022 Part 2 [2].

2.2 Package Claim

This Security Target claims conformance to the assurance package EAL4 augmented and the COMP Package, defined by CC:2022 part 5 [5].

The augmentations to EAL4 are:

- ADV_FSP.5 ‘Complete semi-formal functional specification with additional error information’
- ADV_INT.2 ‘Well-structured internals’
- ADV_TDS.4 ‘Semiformal modular design’

- ALC_CMS.5 ‘Development tools CM coverage’
- ALC_DVS.2 ‘Sufficiency of security measures’
- ALC_TAT.2 ‘Compliance with implementation standards’
- ATE_DPT.3 ‘Testing: modular design’

2.3 PP Claim

This ST claims strict conformance to the following Protection Profile:

Protection Profile [7] **Machine Readable Travel Document with “ICAO Application”, Basic Access Control**	
Version	1.10
Date	25th March 2009
Prepared by	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Identification	PP0055
Approved by	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Registration	BSI-CC-PP-0055-2009
Assurance Level	Common Criteria 3.1 EAL 4 augmented by ALC_DVS.2

The ICAO BAC PP defines the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control and Chip Authentication similar to the Active Authentication in the Technical reports of ‘ICAO Doc 9303’ [9].

This MRTD’s IC does not limit the TOE interfaces to contactless: both contact and contactless interfaces are part of this TOE and the PP content has been enhanced for this purpose.

Additions to the claims from the PP [7] have been added to the related sections of this Security Target and are listed including rationales in section 7.4 of this Security Target.

The Composite Product Package (COMP) is defined in CC:2022 Part 5 [5]

2.4 Rationale Regarding CC:2022

This security target strictly conforms to the Protection Profile [7] with the additional Objective for the TOE, OT.AA_Proof and objective for the Environment, OE.Active_Auth_Key, for the supported *Active Authentication* functionality, specified in ICAO Doc 9303 [9]. However, the PP is compliant to CCv3.1 and this Security Target is compliant with CC:2022 and makes the following adjustments in accordance with the CCRA Transition Policy [24].

The extended components defined in the CCv3.1 compliant PP [7] have been replaced by the components defined in CC:2022 part 2 [2].

Extended Component [7]	CC:2022 Part 2 Component	Justification
FCS_RND.1: ‘Generation of random numbers’	FCS_RNG.1: ‘Random Number Generation’	FCS_RNG.1 is equivalent to FCS_RND.1 since both require random numbers satisfy defined quality metrics
FMT_LIM.1: ‘Limited capabilities’	FMT_LIM.1: ‘Limited capabilities’	FMT_LIM.1 is implemented in CC:2022 with only a minor change in wording
FMT_LIM.2: ‘Limited availability’	FMT_LIM.2: ‘Limited availability’	FMT_LIM.2 is implemented in CC:2022 with the same wording.
FPT_EMSEC.1: ‘TOE emanation’	FPT_EMS.1: ‘TOE emanation’	FMT_EMS.1 is equivalent to the extended component FPT_EMSEC.1 as it addresses requirements related to information leakage via emanation
FCS_COP.1	FCS_COP.1	FCS_RNG.1 is added to the dependencies of FCS_COP.1

Table 5. PP0055 Extended Components in CC:2022

Extended Component [8]	CC:2022 Part 2 Component	Justification
FIA_API.1: ‘Authentication Proof of Identity’	FIA_API.1 ‘Authentication proof of Identity’	FIA_API.1 is implemented in CC:2022 as an authentication proof with additional properties included in the definition refining the PP definition.

Table 6. PP0056 Extended Components in CC:2022

Table 1: PP0056 Extended Components in CC:2022

According to the transition Policy the CCV3.1 component FCS_CKM.4 is now replaced by CC:2022 component FCS_CKM.6.

The SFR dependency analysis is updated in accordance with CC:2022 dependencies and the clarification of CC:2022 Errata [26].

3. Security Problem Definition (ASE_SPD)

Extensions to the Security Problem Definition from the PP [7] are underlined and listed in section 7.4.1.

3.1 Assets

The assets to be protected by the TOE include the User Data on the MRTD's chip.

Logical MRTD sensitive User Data

Sensitive biometric reference data:

- **EF.DG3**: Biometric Finger(s)
- **EF.DG4**: Biometric Eye(s) Iris

Logical MRTD data

The 'ICAO Doc 9303' [9] requires that Basic Inspection Systems must have access to:

- **EF.COM**: Common Data Elements, lists the existing EF with the user data
- **EF.SOD**: Document Security Object according to LDS [9] used by the inspection system for Passive Authentication of the logical MRTD
- **EF.DG1**: document's data (Type, Issuing State or Organization, Number, Expiry Date, Optional Data), holder's data (Name, Nationality, Date of Birth, Sex) and Check Digits
- **EF.DG2**: Encoded Face (Global Interchange Feature)
- **EF.DG5**: Biometric Face
- **EF.DG7**: Displayed Signature or Usual Mark
- **EF.DG8**: Displayed Portrait
- **EF.DG9**: Data Feature(s)
- **EF.DG10**: Structure Feature(s)
- **EF.DG11**: Additional Personal Detail(s)
- **EF.DG12**: Additional Document Detail(s)
- **EF.DG13**: optional Detail(s)
- **EF.DG14**: Security Info (Chip Authentication Public Key Info)
- **EF.DG15**: Active Authentication Public Key Info
- **EF.DG16**: Person(s) to Notify

Due to interoperability reasons with 'ICAO Doc 9303' [9], the TOE specifies the BAC mechanisms with resistance against enhanced basic attack potential granting access to:

- Logical MRTD standard User Data (i.e. Personal Data) of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16) (DG6 is absent),
- Chip Authentication Public Key in EF.DG14,
- Active Authentication Public Key in EF.DG15,

- Document Security Object (SOD) in EF.SOD,
- Common data in EF.COM.

The TOE prevents read access to sensitive User Data

- Sensitive biometric reference data (EF.DG3, EF.DG4).

Authenticity of the MRTD's chip

The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD holder is used by the traveler to prove his possession of a genuine MRTD.

3.2 Subjects

This Security Target considers the following subjects:

S.Manufacturer

The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the user IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

S.Personalizer *Personalization Agent*

The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities: (i) establishing the identity of the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s), (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (v) signing the Document Security Object defined in [9].

S.Country *Country Verifying Certification Authority*

The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.

S.DV *Document Verifier*

The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.

S.Terminal

A terminal is any technical system communicating with the TOE through its physical interfaces.

S.IS	*Inspection system*

A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The **Basic Inspection System** (BIS) (i) contains a terminal for the communication with the MRTD's chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. The **General Inspection System** (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The **Extended Inspection System** (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

S.Holder	*MRTD Holder*

The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

S.Traveler

Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

3.3 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

A.MRTD_Manufact *MRTD manufacturing on steps 5 to 6*

It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

A.MRTD_Delivery *MRTD delivery during steps 5 to 6*

Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

- Procedures shall ensure protection of TOE material/information under delivery and storage.
- Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
- Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

A.Pers_Agent	*Personalization of the MRTD's chip*

The Personalization Agent ensures the correctness of

- the logical MRTD with respect to the MRTD holder,

- the Document Basic Access Keys,
- the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and
- the Document Signer Public Key Certificate (if stored on the MRTD's chip).

The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.Pers_Agent_AA *Personalization of the MRTD's chip including Active Authentication*

The Personalization Agent ensures the correctness of the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip.

The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.Insp_Sys *Inspection Systems for global interoperability*

The Inspection System is used by the border control officer of the receiving State:

- examining an MRTD presented by the traveler and verifying its authenticity and
- verifying the traveler as MRTD holder.

The Basic Inspection System for global interoperability

- includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and
- implements the terminal part of the Basic Access Control [9].

The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System (i) supports the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

A.Insp_Sys_AA *Inspection Systems for global interoperability with Active Authentication*

The Inspection System may also implement the terminal part of the Active Authentication Protocol.

A.BAC-Keys *Cryptographic quality of Basic Access Control Keys*

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [9], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

Application note: *When assessing the MRZ data resp. the BAC keys entropy potential dependencies between these data (especially single items of the MRZ) have to be considered and taken into account. E.g. there might be a direct dependency between the Document Number when chosen consecutively and the issuing date.*

3.4 Threat agent

S.ATTACKER	A threat agent trying (i) to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the printed MRZ data), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD.

Application note: *An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged MRTD. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.*

3.5 Threats

The TOE in collaboration with its IT environment shall avert the threats as specified below.

T.Chip_ID *Identification of MRTD's chip*

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the TOE communication interfaces.

The attacker has enhanced basic attack potential and does not know the optically readable MRZ data printed on the MRTD data page in advance.

Threatened asset is the user anonymity.

T.Skimming *Skimming the logical MRTD*

An attacker imitates an inspection system trying to establish a communication to read the logical MRTD or parts of it via the communication channels of the TOE.

The attacker does not know the optically readable MRZ data printed on the MRTD data page in advance.

Threatened asset is the confidentiality of logical MRTD data.

T.Eavesdropping *Eavesdropping to the communication between TOE and inspection system*

An attacker is listening to an existing communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know these data in advance.

The attacker has enhanced basic attack potential and does not know the optically readable MRZ data printed on the MRTD data page in advance.

Threatened asset is the confidentiality of logical MRTD data.

T.Forgery	*Forgery of data on MRTD's chip*

An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data. This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another chip.

The attacker has enhanced basic attack potential and is in possession of one or more legitimate MRTDs.

Threatened asset is authenticity of logical MRTD data.

T.Counterfeit	*Counterfeit MRTD's chip*

An attacker produces an unauthorised copy or reproduction of a genuine MRTD's chip to be used as part of a counterfeit MRTD. This violates the authenticity of the MRTD's chip used for authentication of a traveler by possession of a MRTD. The attacker may generate a new data set or extract completely or partially the data from a genuine MRTD's chip and copy them on another appropriate chip to imitate this genuine MRTD's chip.

The attacker is in possession of one or more legitimate MRTDs.

Threatened asset is authenticity of logical MRTD data.

The TOE shall avert the threats as specified below.

T.Abuse-Func	*Abuse of Functionality*

An attacker may use functions of the TOE which shall not be used in "Operational Use" phase in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data. This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.

The attacker has enhanced basic attack potential and is in possession of a legitimate MRTD.

Threatened assets are confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

T.Information_Leakage *Information Leakage from MRTD's chip*

An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters which may be derived either from measurements of the communication interfaces (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

The attacker has enhanced basic attack potential and is in possession of a legitimate MRTD.

Threatened asset is confidentiality of logical MRTD and TSF data.

T.Phys-Tamper *Physical Tampering*

An attacker may perform physical probing of the MRTD's chip in order (i) to disclose TSF Data, or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data. The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

The attacker has enhanced basic attack potential and is in possession of a legitimate MRTD.

Threatened assets are confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

T.Malfunction *Malfunction due to Environmental Stress*

An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software. This may be achieved e.g. by operating the MRTD's

chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

The attacker has enhanced basic attack potential and is in possession of a legitimate MRTD.

Threatened assets are confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

3.6 Organisational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

P.Manufact	*Manufacturing of the MRTD's chip*

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

P.Personalization	*Personalization of the MRTD by issuing State or Organization only*

The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical MRTD with respect to the MRTD holder. The personalization of the MRTD for the holder is performed by an agent authorized by the issuing State or Organization only.

P.Personal_Data	*Personal data protection policy*

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4)3 and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [9].

Application note: *The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [9]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.*

4. Security Objectives (ASE_OBJ)

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development and production environment and security objectives for the operational environment.

Extensions to the security objectives from the PP [7] are underlined and listed in section 7.4.2.

4.1 SOs for the TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE.

OT.AC_Pers	*Access Control for Personalization of logical MRTD*

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [9] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

Application note: *The OT.AC_Pers implies that*

(1) the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) cannot be changed by write access after personalization,

(2) the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the "Operational Use" phase is optional.

OT.Data_Int	*Integrity of personal data*

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure the integrity of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

OT.Data_Conf	*Confidentiality of personal data*

The TOE must ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

Application note: *The traveler grants the authorization for reading the personal data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 to the inspection system by presenting the*

MRTD. The MRTD's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys.The security objective OT.Data_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication. The Document Basic Access Keys are derived from the MRZ data defined by the TOE environment and are loaded into the TOE by the Personalization Agent. Therefore the sufficient quality of these keys has to result from the MRZ data's entropy. Any attack based on decision of the 'ICAO Doc 9303' [9] that the inspection system derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this TOE. Thus the read access must be prevented even in case of a successful BAC Authentication.

OT.Identification	*Identification and Authentication of the TOE*

The TOE must provide means to store IC Identification and Pre-Personalization Data in its nonvolatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRTD". The storage of the Pre- Personalization data includes writing of the Personalization Agent Key(s). In Phase 4 "Operational Use" the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

Application note: *The TOE security objective OT.Identification addresses security features of the TOE to support the lifecycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 "Manufacturing" and for traceability and/or to secure shipment of the TOE from Phase 2 "Manufacturing" into the Phase 3 "Personalization of the MRTD". The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 "Operational Use" the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the physical interfaces before successful authentication as Basic Inspection System or as Personalization Agent.*

OT.AA_Proof	*Proof of MRTD's chip authenticity by Active Authentication*

The TOE may support the Basic Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [9].

The following TOE security objectives address the protection provided by the MRTD's chip independent of the TOE environment.

OT.Prot_Abuse-Func	*Protection against Abuse of Functionality*

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to (i) disclose critical User Data, (ii) manipulate critical User Data of the IC Embedded Software, (iii) manipulate Soft-coded IC Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.

Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

OT.Prot_Inf_Leak	*Protection against Information Leakage*

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD's chip

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines and
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

Application note: *This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.*

OT.Prot_Phys-Tamper	*Protection against Physical Tampering*

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with high attack potential by means of

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data)
- with a prior
- reverse-engineering to understand the design and its properties and functions.

OT.Prot_Malfunction	*Protection against Malfunctions*

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested.

This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

Application note: *A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE´s internals.*

4.2 SOs for the Environment

4.2.1 Issuing State or Organization

The issuing State or Organization will implement the following security objectives of the TOE environment.

OE.MRTD_Manufact	*Protection of the MRTD Manufacturing*

Appropriate functionality testing of the TOE shall be used in step 5 to 6.

During all manufacturing and test operations, security procedures shall be used through steps 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

OE.MRTD_Delivery	*Protection of the MRTD delivery*

Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

- non-disclosure of any security relevant information,
- identification of the element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- physical protection to prevent external damage,
- secure storage and handling procedures (including rejected TOE's),
- traceability of TOE during delivery including the following parameters:
  - origin and shipment details,
  - reception, reception acknowledgement,
  - location material/information.

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process.

Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

OE.Personalization	*Personalization of logical MRTD*

The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization (i) establish the correct identity of the holder and create biographical data for the MRTD, (ii) enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and (iii) personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

OE.Pass_Auth_Sign	*Authentication of logical MRTD by Signature*

The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute

the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [9].

OE.BAC-Keys	*Cryptographic quality of Basic Access Control Keys*

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [9] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.

OE.Active_Auth_Key	*Active Authentication Key*

The issuing State or Organization may establish the necessary public key infrastructure in order to:

- Generate the MRTD's Active Authentication Key Pair,
- Sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 and
- Support inspection systems of receiving States or Organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object

4.2.2 Receiving State or Organization

The receiving State or Organization will implement the following security objectives of the TOE environment.

OE.Exam_MRTD	*Examination of the MRTD passport book*

The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [9].

OE.Exam_MRTD_AA	*Examination of the MRTD passport book using Active Authentication*

During examination of the MRTD presented by the traveler, the basic inspection system may follow the Active Authentication Protocol to verify the authenticity of the presented MRTD's chip.

OE.Passive_Auth_Verif	*Verification by Passive Authentication*

The border control officer of the receiving State uses the inspection system to verify the traveler as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and Organizations must manage the Country Signing Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

OE.Prot_Logical_MRTD	*Protection of data from the logical MRTD*

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

4.3 Security objectives rationale

All the security objectives described in the ST are traced back to items described in the TOE security environment and any items in the TOE security environment are covered by those security objectives appropriately.

4.3.1 Security Objectives Coverage

The following able indicates that all security objectives of the TOE are traced back to threats and/or organizational security policies and that all security objectives of the environment are traced back to threats, organizational security policies and/or assumptions.

Threats Assumptions Policies / Security objectives	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.AA_Proof	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Exam_MRTD	OE.Exam_MRTD_AA	OE.Active_Auth_Key	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
T.Chip_ID				X										X					
T.Skimming			X											X					
T.Eavesdropping			X																
T.Forgery	X	X					X						X		X			X	
T.Counterfeit					X	X	X	X	X							X	X		
T.Abuse-Func					X							X							
T.Information_Leakage						X													
T.Phys-Tamper							X												
T.Malfunction								X											
P.Manufact				X															
P.Personalization	X			X								X							
P.Personal_Data		X	X																
A.MRTD_Manufact										X									
A.MRTD_Delivery											X								
A.Pers_Agent												X							
A.Pers_Agent_AA												X							

Threats Assumptions Policies / Security objectives	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.AA_Proof	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Exam_MRTD	OE.Exam_MRTD_AA	OE.Active_Auth_Key	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
A.Insp_Sys															X				X
A.Insp_Sys_AA																X			
A.BAC-Keys														X					

Table 7. Security Environment to Security Objectives Mapping

4.3.2 Security Objectives Sufficiency

4.3.2.1 Policies and Security Objective Sufficiency

The OSP **P.Manufact "Manufacturing of the MRTD's chip"** requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data as being fulfilled by OT.Identification.

The OSP **P.Personalization "Personalization of the MRTD by issuing State or Organization only"** addresses the (i) the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment OE.Personalization "Personalization of logical MRTD", and (ii) the access control for the user data and TSF data as described by the security objective OT.AC_Pers "Access Control for Personalization of logical MRTD". Note the manufacturer equips the TOE with the Personalization Agent Key(s) according to OT.Identification "Identification and Authentication of the TOE". The security objective OT.AC_Pers limits the management of TSF data and management of TSF to the Personalization Agent.

The OSP **P.Personal_Data "Personal data protection policy"** requires the TOE (i) to support the protection of the confidentiality of the logical MRTD by means of the Basic Access Control and (ii) enforce the access control for reading as decided by the issuing State or Organization. This policy is implemented by the security objectives OT.Data_Int "Integrity of personal data" describing the unconditional protection of the integrity of the stored data and during transmission. The security objective OT.Data_Conf "Confidentiality of personal data" describes the protection of the confidentiality.

4.3.2.2 Threats and Security Objective Sufficiency

The threat **T.Chip_ID "Identification of MRTD's chip"** addresses the trace of the MRTD movement by identifying remotely the MRTD's chip through the physical communication interface. This threat is countered as described by the security objective OT.Identification by Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment OE.BAC-Keys.

The threat **T.Skimming "Skimming digital MRZ data or the digital portrait"** and **T.Eavesdropping "Eavesdropping to the communication between TOE and inspection system"** address the reading of the logical MRTD trough the physical communication interface or listening the communication between the MRTD's chip and a terminal. This threat is countered by the security objective OT.Data_Conf "Confidentiality

of personal data” through Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment OE.BAC-Keys.

The threat **T.Forgery “Forgery of data on MRTD’s chip”** addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective OT.AC_Pers “Access Control for Personalization of logical MRTD“ requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity of the stored logical MRTD according the security objective OT.Data_Int “Integrity of personal data” and OT.Prot_Phys-Tamper “Protection against Physical Tampering”. The examination of the presented MRTD passport book according to OE.Exam_MRTD “Examination of the MRTD passport book” shall ensure that passport book does not contain a sensitive chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to OE.Pass_Auth_Sign “Authentication of logical MRTD by Signature” and verified by the inspection system according to OE.Passive_Auth_Verif “Verification by Passive Authentication”.

The threat **T.Abuse-Func “Abuse of Functionality”** addresses attacks using the MRTD’s chip as production material for the MRTD and misuse of the functions for personalization in the operational state after delivery to MRTD holder to disclose or to manipulate the logical MRTD. This threat is countered by OT.Prot_Abuse-Func “Protection against Abuse of Functionality”. Additionally this objective is supported by the security objective for the TOE environment: OE.Personalization “Personalization of logical MRTD” ensuring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to MRTD holder are enabled according to the intended use of the TOE.

The threats **T.Information_Leakage “Information Leakage from MRTD’s chip”**, **T.Phys-Tamper “Physical Tampering”** and **T.Malfunction “Malfunction due to Environmental Stress”** are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives OT.Prot_Inf_Leak “Protection against Information Leakage”, OT.Prot_Phys-Tamper “Protection against Physical Tampering” and OT.Prot_Malfunction “Protection against Malfunctions”.

The threat **T.Counterfeit “MRTD’s chip”** addresses the attack of unauthorised copy or reproduction of the genuine MRTD chip. This attack is thwarted by a set of objectives that ensure that MRTD’s chip data are not copied from the TOE: OT.Prot_Abuse-Func, OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper, and OT.Prot_Malfunction. In addition, when the MRTD supports Active Authentication, the TOE addresses additional protections against this threat: OT.AA_Proof “Proof of MRTD’s chip authenticity by Active Authentication”, OE.Exam_MRTD_AA “Examination of the MRTD passport book using Active Authentication” and OE.Active_Auth_Key “Active Authentication Key” all participate in the detection of counterfeit MRTD’s chip by the inspection system.

These objectives ensure that no data may be copied from the TOE.

4.3.2.3 Assumptions and Security Objective Sufficiency

The assumption **A.MRTD_Manufact “MRTD manufacturing on step 5 to 6”** is covered by the security objective for the TOE environment OE.MRTD_Manufact “Protection of the

MRTD Manufacturing" that requires to use security procedures during all manufacturing steps.

The assumption **A.MRTD_Delivery "MRTD delivery during step 5 to 6"** is covered by the security objective for the TOE environment OE.MRTD_ Delivery "Protection of the MRTD delivery" that requires to use security procedures during delivery steps of the MRTD.

The assumption **A.Pers_Agent "Personalization of the MRTD's chip"** is covered by the security objective for the TOE environment OE.Personalization "Personalization of logical MRTD" including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data.

The assumption **A.Pers_Agent_AA "Personalization of the MRTD's chip including Active Authentication"** is covered by the security objective for the TOE environment OE.Personalization "Personalization of logical MRTD" including the protection with a digital signature (SOD signing), the storage of the MRTD holder personal data and the support of Active Authentication Protocol according to the decision of the issuing State or Organization.

The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys "Inspection Systems for global interoperability"** is covered by the security objectives for the TOE environment OE.Exam_MRTD "Examination of the MRTD passport book". The security objectives for the TOE environment OE.Prot_Logical_MRTD "Protection of data from the logical MRTD" will require the Basic Inspection System to implement the Basic Access Control and to protect the logical MRTD data during the transmission and the internal handling.

The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys_AA "Inspection Systems for global interoperability with Active Authentication"** is covered by the security objectives for the TOE environment OE.Exam_MRTD_AA "Examination of the MRTD passport book using Active Authentication" which requires the Basic Inspection System to implement and to enforce Active Authentication of the MRTD as part of the MRTD's inspection.

The assumption **A.BAC-Keys "Cryptographic quality of Basic Access Control Keys"** is directly covered by the security objective for the TOE environment OE.BAC-Keys "Cryptographic quality of Basic Access Control Keys" ensuring the sufficient key quality to be provided by the issuing State or Organization.

5. Extended Components Definition (ASE_ECD)

This ST uses components defined as extensions to CC part 2 in the claimed ICAO BAC PP [7], and from ICAO EAC PP for the Active Authentication functionality, which is compliant to CC version 3.1 however in accordance with the CC:2022 Transition Policy [24], where applicable are replaced by SFRs now defined in CC:2022 Part 2 [2]:

Defined in Protection Profile	CC:2022 equivalent
FAU_SAS.1: 'Audit data storage'	n/a
FCS_RND.1: 'Generation of random numbers'	FCS_RNG.1: 'Random Number Generation'
FMT_LIM.1: 'Limited capabilities'	FMT_LIM.1: 'Limited capabilities'
FMT_LIM.2: 'Limited availability'	FMT_LIM.2: 'Limited availability'
FPT_EMSEC.1: 'TOE emanation'	FPT_EMS.1: 'TOE emanation'
FIA_API.1: 'Authentication Proof of Identity'	FIA_API.1 'Authentication proof of Identity'

Table 8. PP Extended Component Definitions

5.1 Audit data storage (FAU_SAS)

To define the security functional requirements of the TOE, a sensitive family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

The family "Audit data storage (FAU_SAS)" is specified as follows.

FAU_SAS Audit data storage

Family behavior

This family defines functional requirements for the storage of audit data.

Component leveling:

	FAU_SAS Audit data storage	1
FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.	

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	**The TSF shall provide [assignment: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.**

5.2 Security Requirements (ASE_REQ)

This chapter gives the security functional requirements and the security assurance requirements for the TOE.

Some security functional requirements represent extensions to [2].

Operations for assignment, selection and refinement have been made and are designated by an underline (e.g. none), in addition, where operations that were uncompleted in the PP [7] are also identified by *italic underlined* type.

The TOE security assurance requirements statement given in section 5.4 is drawn from the security assurance components from Common Criteria part 3 [3].

The definition of the subjects “Manufacturer”, “Personalization Agent”, “Basic Inspection System” and “Terminal” used in the following chapter is given in section 3.2. Note, that all these subjects are acting for homonymous external entities. All used objects are defined in section 8. The operations “write”, “read”, “modify”, and “disable read access” are used in accordance with the general linguistic usage. The operations “transmit”, “receive” and “authenticate” are originally taken from [2].

Definition of security attributes:

Security attribute	Values	Meaning
Terminal authentication status	none (any Terminal)	default role (i.e. without authorisation after start-up)
	Basic Inspection System	Terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2.
	Personalisation Agent	Terminal is authenticated as Personalisation Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2.

The following table provides an overview of the keys used:

Name	Data
Active Authentication Key Pair	The Active Authentication asymmetric Key Pair (KPr_{AA}, KPu_{AA}) is used for the Active Authentication Protocol: allowing the chip to be authenticated as genuine by the inspection system.
Active Authentication Private Key (KPr_{AA})	The Active Authentication Private Key (KPr_{AA}) is used by the TOE to be authenticated as a genuine MRTD’s chip by the inspection system. It is part of the TSF data.
Active Authentication Public Key (KPu_{AA})	The Active Authentication Public Key (KPu_{AA}) is stored in the EF.DG15 Active Authentication Public Key of the TOE’s logical MRTD and used by the inspection system for Active Authentication of the MRTD’s chip. It is part of the user data provided by the TOE for the IT environment.
Country Signing Certification	Country Signing Certification Authority of the issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the

Name	Data
Authority Key Pair	signature will be verified by receiving State or Organization (e.g. a Basic Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organization signs the Document Security Object of the logical MRTD with the Document Signer Private Key and the signature will be verified by a Basic Inspection Systems of the receiving State or Organization with the Document Signer Public Key.
Document Basic Access Keys	The Document Basic Access Key is created by the Personalization Agent, loaded to the TOE, and used for mutual authentication and key agreement for secure messaging between the Basic Inspection System and the MRTD's chip.
BAC Session Keys	Secure messaging TDES key and Retail-MAC key agreed between the TOE and a Basic Inspection System in result of the Basic Access Control Authentication Protocol.

5.3 TOE Security Functional Requirements

5.3.1 Security Audit (FAU)

5.3.1.1 Audit Storage (FAU_SAS.1)

FAU_SAS.1.1 The TSF shall provide the Manufacturer with the capability to store the IC Identification Data in the audit records.

Application note: *The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS).*

5.3.2 Cryptographic support (FCS)

Function		Algorithm	Key Size(s)
Basic Access	Authentication	TDES CBC	112 bits
Active Authentication	Signature generation	RSA signature based on ISO9796-2 scheme 1 [11]	1024, 1280, 1536, 2048 and 4096
		ECDSA / ECC of GF(p) based on [19]	224, 256, 384 and 521
Secure Messaging	ENC/DEC	TDES CBC	112 bits
	MAC	Retail MAC	112 bits

5.3.2.1 Cryptographic key generation (FCS_CKM.1)

→ Generation of Document Basic Access Keys by the TOE

FCS_CKM.1.1/ BAC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [9].

Application note: *The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [9], normative appendix 5, A5.2, produces agreed parameters to generate the Triple- DES (TDES) key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [9], Normative appendix A5.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RNG.1.*

→ Generation of Active Authentication Key Pair by the TOE

FCS_CKM.1.1/ KP The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA and ECC key pair generation* and specified cryptographic key sizes *1024-1280-1536-2048-4096 bit in case of RSA and 224, 256, 384 and*

521 bit in case of ECC that meet the following: *PKCS#1 v1.5 as per Algorithms and parameters for algorithms [15]*.

Application note: *The component FMT_MTD.1/AAPK defines an operation "create" that means that the Active Authentication Private Key is generated by the TOE itself. This resulted in this instantiation of the component FCS_CKM.1 as SFR for this key generation.*

5.3.2.2 Cryptographic key destruction (FCS_CKM.6)

FCS_CKM.6.1	The TSF shall destroy *Personalization Agent Authentication Keys, Personalization Session Keys, BAC Session Keys, Active Authentication Private Keys*[1] when *no longer needed*[2].
FCS_CKM.6.2	The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method *physical deletion by overwriting the memory data with zeros* [3] that meets the following: *none*[4])

Application note: *The TOE shall destroy the TDES encryption key and the Retail-MAC message authentication keys for secure messaging.*

5.3.2.3 Cryptographic operation (FCS_COP.1)

→ Hashing for Key Derivation

FCS_COP.1.1/ SHA	The TSF shall perform hashing in accordance with a specified cryptographic algorithm *SHA-1 or SHA-256* and cryptographic key sizes none that meet the following: *FIPS 180-2 [12]*.

Application note: *This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA_UAU.4) according to [9].*

→ SM Encrypt/Decrypt

FCS_COP.1.1/ ENC	The TSF shall perform secure messaging (BAC) – encryption and decryption in accordance with a specified cryptographic algorithm TDES in CBC mode and cryptographic key sizes 112 bit that meet the following: FIPS 46-3 [13] and [9], A5.3.

Application note: *The TOE implements the cryptographic primitives (e.g. TDES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol according to the FCS_CKM.1. Furthermore the SFR is used for authentication attempts of a terminal as Personalization Agent by means of the symmetric authentication mechanism.*

→ Authentication

1. [1] [assignment: list of cryptographic keys (including keying material)]
2. [2] [selection: no longer needed, [assignment: other circumstances for key or keying material destruction]].
3. [3] [assignment: cryptographic key destruction method]
4. [4] [assignment: list of standards]

FCS_COP.1.1/ AUTH	The TSF shall perform symmetric authentication – encryption and decryption in accordance with a specified cryptographic algorithm *TDES, AES* and cryptographic key sizes *112 (TDES), 128, 192, 256 (AES) bits* that meet the following: *FIPS 46-3 [13] (TDES), FIPS 197 [23] (AES)*.

Application note: *This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).*

→ SM - MAC

FCS_COP.1.1/ MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm Retail MAC and cryptographic key sizes 112 bits that meet the following: 'ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2).

Application note: *This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.*

→ Signature generation

FCS_COP.1.1/ SIG_GEN	The TSF shall perform *digital signature generation* in accordance with a specified cryptographic algorithm *RSA and ECDSA* and cryptographic key sizes *RSA 1024-1280-1536-2048-4096 bits and ECC NIST/Brainpool 224, 256, 384, 512 and 521 in case of ECC* that meet the following: *ISO/IEC 9796-2 [11](RSA) and ANSI x9.62 (ECC) [21]*

Application note: *For signature generation in the Active Authentication mechanism, the TOE uses ISO/IEC 9796-2 compliant cryptography (scheme 1).*

5.3.2.4 Random Number Generation (FCS_RNG.1)

FCS_RNG.1.1	The TSF shall provide a *hybrid deterministic* [5] random number generator that implements: *AIS31 class DRG.4*[6].
FCS_RNG.1.2	The TSF shall provide *numbers* [7]that meet *AIS31 Class DRG.4*[8].

5. [5][selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]
6. [6] [assignment: list of security capabilities]
7. [7] [selection: bits, octets of bots, numbers [assignment: format of the numbers]
8. [8] [assignment: a defined quality metric]

Application note: *This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.*

Application Note: This functionality is provided by the certified JCOP, see *[17]*

5.3.3 User data protection (FDP)

5.3.3.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the Basic Access Control SFP on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD.

5.3.3.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the Basic Access Control SFP to objects based on the following:

1. Subjects:
   a. Personalization Agent,
   b. Basic Inspection System
   c. Terminal,
2. Objects:
   a. data EF.DG1 to EF.DG16 of the logical MRTD,
   b. data in EF.COM,
   c. data in EF.SOD,
3. Security attributes:
   a. authentication status of terminals.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,
2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the rule:

1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.
2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.
3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.

Application note: *The inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this TOE (cf. [11] for details).*

5.3.3.3 Basic data exchange confidentiality (FDP_UCT.1)

Application note: *FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and*

message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

FDP_UCT.1.1 The TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorised disclosure.

5.3.3.4 Data exchange integrity (FDP_UIT.1)

Application note: *See application in FDP_UCT.1.*

FDP_UIT.1.1 The TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred.

5.3.4 Identification and authentication (FIA)

The following table provides an overview on the authentication mechanisms used:

Name	SFR for the TOE	Cryptography
Basic Access Control Authentication Mechanism	FIA_UAU.4, FIA_UAU.6	TDES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agent	FIA_UAU.4	TDES with 112 bit keys (cf. FCS_COP.1/AUTH)
Active Authentication	FIA_API.1, FIA_UAU.4	RSA signature based on ISO9796-2 scheme 1, with Keys 1024, 1280, 1536, 2048 bits (cf. FCS_COP.1.1/ SIG_GEN)

5.3.4.1 Authentication Failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within 1 of consecutive* unsuccessful authentication attempts occur related to *failure of a BAC Authentication*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall *send the response to the authentication request with exponentially increasing time delays until the correct password is used*.

Application note: *The terminal challenge eIFD and the TSF response eICC are described in [10]. The refinement by inclusion of the word "consecutive" allows the TSF to return to normal operation of the BAC authentication protocol (without time out) after successful run of the BAC authentication protocol. The unsuccessful*

authentication attempt shall be stored in non-volatile memory in the TOE thus the "consecutive unsuccessful authentication attempts" are count independent on power-on sessions but reset to zero after successful authentication only.

5.3.4.2 Authentication Proof of Identity (FIA_API.1)

FIA_API.1.1 The TSF shall provide an *Active Authentication Protocol according to [9]*[9] to prove the identity of the *TOE*[10] by including the following properties *Active Authentication Public Key (EF.DG.15)* [11]to an external entity

Application note: *The TOE may implement the Active Authentication Mechanism specified in [9] Part 1 Appendix 4 to section IV. This mechanism is a challenge response protocol where TOE challenge response is calculated being digital signature over the terminal's 8 bytes nonce.*

5.3.4.3 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow

1. to read the Initialization Data in Phase 2 "Manufacturing",
2. to read the random identifier in Phase 3 "Personalization of the MRTD",
3. to read the random identifier in Phase 4 "Operational Use"

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.

Application note: *The Basic Inspection System and the Personalization Agent authenticate themselves.*

5.3.4.4 Single-use authentication mechanisms (FIA_UAU.4)

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to

1. Basic Access Control Authentication Mechanism,
2. Authentication Mechanism based on *TDES*,
3. *Active Authentication Protocol*.

Application note: *The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.*

Application note: *The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [9]. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip authenticates to the terminal in the second step. In this second step the MRTD's chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys.*

9. [9] [assignment: authentication mechanism]
10. [10] [assignment: authorized user or rule]
11. [11] [assignment: list of properties]

Therefore the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfil the security objective OT.Identification and to prevent T.Chip_ID.

5.3.4.5 Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide

1. Basic Access Control Authentication Mechanism,
2. Symmetric Authentication Mechanism based on *TDES*

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules:

1. The TOE accepts the authentication attempt as Personalization Agent by *the Symmetric Authentication Mechanism with Personalization Agent Key*.
2. the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys

Application note: *The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys*

5.3.4.6 Re-authenticating (FIA_UAU.6)

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism.

Application note: *The Basic Access Control Mechanism specified in [9] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.*

Application note: *Note that in case the TOE should also fulfil [8] the BAC communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the BAC based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the BAC communication*

but are protected by a more secure communication channel established after a more advanced authentication process.

5.3.4.7 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow

1. to read the Initialization Data in Phase 2 “Manufacturing”,
2. to read the random identifier in Phase 3 “Personalization of the MRTD”,
3. to read the random identifier in Phase 4 “Operational Use”

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.

Application note: *The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 “Manufacturing”. The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the MRTD”. The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System.*

Application note: *In the “Operational Use” phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD’s chip use a randomly chosen identifier for the communication channel to allow the terminal to communicate with more than one RFID. This identifier is randomly selected and it does not violate the OT.Identification.*

5.3.5 Security management (FMT)

5.3.5.1 Limited capabilities (FMT_LIM.1)

FMT_LIM.1.1 The TSF shall limit its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced:

Deploying Test Features after TOE Delivery does not allow,

1. User Data to be disclosed or manipulated
2. TSF data to be disclosed or manipulated
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks.

5.3.5.2 Limited availability (FMT_LIM.2)

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced:

Deploying Test Features after TOE Delivery does not allow,

1. User Data to be disclosed or manipulated,
2. TSF data to be disclosed or manipulated
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered
5. which may enable other attacks.

Application note: *The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.*
Note that the term "software" in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

5.3.5.3 Management of TSF data (FMT_MTD.1)

→ Writing of Initialization Data and Pre-personalization Data

FMT_MTD.1.1/ INI_ENA The TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer.

Application note: *The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.*

→ Disabling of Read Access to Initialization Data and Pre-personalization Data

FMT_MTD.1.1/ INI_DIS The TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent.

Application note: *According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 "Manufacturing" but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 "personalization" but is not needed and may be misused in the Phase 4 "Operational Use". Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.*

→ Key Write

FMT_MTD.1.1/ KEY_WRITE	The TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent.

Application note: *The Country Verifying Certification Authority Public Key is the TSF data for verification of the certificates of the Document Verifier and the Extended Inspection Systems including the access rights for the Extended Access Control.*

→ Key Read

FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to read the Document Basic Access Keys, *Active Authentication Private Key* and Personalization Agent Keys to none.

Application note: *The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.*

→ Active Authentication Private Key

FMT_MTD.1.1/ AAPK	The TSF shall restrict the ability to *create* the *Active Authentication Private Key* to *the Terminal*.

Application note: *The verb "create" means here that the Terminal (after successful authentication of the Personalization Agent) is requesting the creation of the Active Authentication Key on the TOE and is requesting the secure generation of the Active Authentication Private Key by the TOE itself. See the instantiation of the component FCS_CKM.1 as SFR for this key generation.*

5.3.5.4 Specifications of Management Functions (FMT_SMF.1)

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: 1. Initialization, 2. Pre-personalization, 3. Personalization, 4. *Configuration.*

5.3.5.5 Security roles (FMT_SMR.1)

FMT_SMR.1.1	The TSF shall maintain the roles 1. Manufacturer, 2. Personalization Agent, 3. Basic Inspection System.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

5.3.6 Protection of the TSF (FPT)

5.3.6.1 TOE Emanation (FPT_EMS.1)

FPT_EMS.1.1	The TSF shall ensure that the TOE does not emit emissions over its attack surface in such amount that these emissions enable access to TSF data and user data as specified in Table
Application note: *The TOE prevents attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal*	

operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD's chip provides a smart card contactless interface but may have also (not used by the terminal but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

ID	Emissions	Attack Surface	TSF Data	User Data
1	[assignment: list of types of emissions]	[assignment: list of types of attack surface]	[assignment: list of types of TSF data]	[assignment: list of types of user data]
	Audio frequencies, Radio frequencies, information on power consumption, electromagnetic radiation, and timing information	Travel document contactless/contact interface and circuit contacts	Chip Authentication session Keys, BAC session Keys(BAC-K_{MAC}, BAC-K_{ENC}), Personlization Agent Session Keys	Personalization Agent Keys, Document Basic Access Keys(s), Active Authentication Private Key

5.3.6.2 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

1. Exposure to out-of-range operating conditions where therefore a malfunction could occur,
2. failure detected by TSF according to FPT_TST.1.

5.3.6.3 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist Physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced.

Application note: *The TOE implements appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.*

Application note: *The SFRs "Non-bypassability of the TSF FPT_RVM.1" and "TSF domain separation FPT_SEP.1" are no longer part of [2]. These requirements are now an implicit part of the assurance requirement ADV_ARC.1.*

5.3.6.4 TSF testing (FPT_TST.1)

FPT_TST.1.1	The TSF shall run a suite of self tests *during initial start-up* to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Application note: *self test for the verification of the integrity of stored TSF executable code are executed during initial start-up in the Phase 3 "Personalization" and Phase 4 "Operational Use".*

5.4 TOE Security Assurance Requirements

TOE Security Assurance Requirements as stated in section 6.2 of the claimed PP [7].

The augmentations compared to the CC V3.1 package for EAL4 are:

- ADV_FSP: augmented from 4 to 5
- ADV_INT: added at level 2
- ADV_TDS: augmented from 3 to 4
- ALC_CMS: augmented from 4 to 5
- ALC_DVS: augmented from 1 to 2
- ALC_TAT: augmented from 1 to 2
- ATE_DPT: augmented from 1 to 3

5.4.1 SARs Measures

The assurance measures that satisfy the TOE security assurance requirements are the following:

Assurance Class	Component	Description
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.5	**Complete Semi-formal functional specification with additional error information**
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	**Well-structured internals**
	ADV_TDS.4	**Semi-formal modular design**

Assurance Class	Component	Description
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Lifecycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.5	**Development tools CM coverage**
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	**Sufficiency of security measures**
	ALC_LCD.1	Developer defined lifecycle model
	ALC_TAT.2	**Compliance with implementation standards**
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Test	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	**Testing: modular design**
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3	Methodical vulnerability analysis

Table 9. Assurance Requirements: EAL 4 augmented

Class	Component	Description
ASE	ASE_COMP.1	Consistency of Security Target
ADV	ADV_COMP.1	Design compliance with the base component-related user guidance, ETR for composite evaluation and report of the base component evaluation authority
ALC	ALC_COMP.1	Integration of the dependent component into the related base component and consistency check for delivery and acceptance procedures
ATE	ATE_COMP.1	Composite product functional testing
AVA	AVA_COMP/1	Composite product vulnerability assessment

Table 10. Assurance Components of COMP Package

5.4.2 SARs Rationale

The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though

rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

Augmentation results from the selection of:

ADV_FSP.5 Complete Semi-formal functional specification with additional error information

The selection of the component ADV_FSP.5 provides a better coverage of the functional specification with semi-formal modelling and additional error information.

The component ADV_FSP.5 has the following dependencies: ADV_TDS.4 Semi-formal modular design and ADV_IMP.1 Implementation representation of the TSF.

ADV_INT.2 Well-structured internals

The selection of the component ADV_INT.2 provides additional information regarding the TSF internals by analysing the complexity to justify it is well-structured.

The component ADV_INT.2 has the following dependencies: ADV_IMP.1 Implementation representation of the TSF, ADV_TDS.4 Semi-formal modular design, and ALC_TAT.1 Well-defined development tools.

ADV_TDS.4 Semi-formal modular design

The selection of the component ADV_TDS.4 provides enhanced design of the TOE introducing semi-formal modelling of the subsystems and differentiating the roles of the modules regarding each TSF.

The component ADV_TDS.4 has the following dependency: ADV_FSP.5 Complete semi-formal functional specification with additional error information.

ALC_DVS.2 Life-cycle support- Sufficiency of security measures

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD’s development and manufacturing especially for the secure handling of the MRTD’s material.

The component ALC_DVS.2 has no dependencies.

ALC_CMS.5 Development tools CM coverage

The selection of the component ALC_CMS.5 provides improved configuration management by covering the development tools (compiler options, build options etc…).

The component ALC_CMS.5 has no dependencies.

ALC_TAT.2 Compliance with implementation standards

The selection of the component ALC_TAT.2 provides additional information on the implementation standards applied by the developer.

The component ALC_TAT.2 has the following dependency: ADV_IMP.1 Implementation representation of the TSF.

ATE_DPT.3 Testing: modular design

The selection of the component ATE_DPT.3 provides improved testing depth by requiring modular testing versus testing focused on the TSF-enforcing modules.

The component ATE_DPT.3 has the following dependencies: ADV_ARC.1 Security architecture description, ADV_TDS.4 Semiformal modular design, and ATE_FUN.1 Functional testing.

All of these are met or exceeded in the EAL4 assurance package.

5.5 Security Requirements Rationale

5.5.1 Security Requirement Coverage

The following able indicates the association of the SFRs and the SOs of the TOE. The Security Requirements of the TOE correspond to at least one security objective of the TOE. Moreover, some requirements correspond to the security objectives of the TOE in combination with other objectives.

TOE Security Functional Requirement / TOE Security objectives	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.AA_Proof
FAU_SAS.1				X					
FCS_CKM.1/ BAC	X	X	X						
FCS_CKM.1/ KP									X
FCS_CKM.6	X		X						
FCS_COP.1/ SHA	X	X	X						X
FCS_COP.1/ ENC	X	X	X						
FCS_COP.1/ AUTH	X	X							
FCS_COP.1/ MAC	X	X	X						
FCS_COP.1/ SIG_GEN									X
FCS_RNG.1	X	X	X						X
FDP_ACC.1	X	X	X						
FDP_ACF.1	X	X	X						
FDP_UCT.1	X	X	X						
FDP_UIT.1	X	X	X						
FIA_API.1									X
FIA_UID.1			X	X					
FIA_UAU.1			X	X					
FIA_UAU.4	X	X	X						
FIA_UAU.5	X	X	X						
FIA_UAU.6	X	X	X						
FIA_AFL.1			X	X					
FMT_LIM.1					X				
FMT_LIM.2					X				
FMT_MTD.1/ INI_ENA				X					
FMT_MTD.1/ INI_DIS				X					

TOE Security Functional Requirement / TOE Security objectives	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.AA_Proof
FMT_MTD.1/ KEY_WRITE	X	X	X						
FMT_MTD.1/ KEY_READ	X	X	X						
FMT_MTD.1/ AAPK									X
FMT_SMF.1	X	X	X						
FMT_SMR.1	X	X	X						
FPT_EMSEC.1	X					X			
FPT_FLS.1	X					X		X	
FPT_PHP.3	X					X	X		
FPT_TST.1						X		X	

Table 11. Functional Requirement to TOE Security Objective Mapping

5.5.2 Security Requirements Sufficiency

5.5.2.1 TOE Security Requirements Sufficiency

OT.AC_Pers (Access Control for Personalization of logical MRTD) addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1 and FDP_ACF.1 as follows: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated either by using the BAC mechanism (FCS_CKM.1, FCS_COP.1/SHA, FCS_RNG.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the personalization key or for reasons of interoperability with the [8] by using the symmetric authentication mechanism (FCS_COP.1/ AUTH).

In case of using the BAC mechanism the SFR FIA_UAU.6 describes the re-authentication and FDP_UCT.1 and FDP_UIT.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RNG.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC for the ENC_MAC_Mode.

The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) setting the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FCS_CKM.6, FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

OT.Data_Int (Integrity of personal data) requires the TOE to protect the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6 using either FCS_COP.1/ENC and FCS_COP.1/MAC or FCS_COP.1/AUTH.

OT.Data_Int (Integrity of personal data) requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data by means of the BAC mechanism. The SFR FIA_UAU.6, FDP_UCT.1 and FDP_UIT.1 requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RNG.1 (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ.

OT.Identification (Identification and Authentication of the TOE) address the storage of the IC Identification Data uniquely identifying the MRTD's chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU_SAS.1.

Furthermore, the TOE shall identify itself only to a successful authenticated Basic Inspection System in Phase 4 "Operational Use". The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 "Operational Use" violates the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD's chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt (cf. Application note 30). In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

OT.Data_Conf (Confidentiality of personal data) requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: the successful authenticated Personalization Agent is allowed to read the data of the logical MRTD (EF.DG1 to EF.DG16). The successful authenticated Basic Inspection System is allowed to read the data of the logical MRTD (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR

FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys).

The SFR FIA_UAU.4 prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5 enforces the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6 requests secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/ENC and FCS_COP.1/MAC (cf. the SFR FDP_UCT.1 and FDP_UIT.1). (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1, FCS_CKM.6, FCS_COP.1/SHA and FCS_RNG.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

Note, neither the security objective OT.Data_Conf nor the SFR FIA_UAU.5 requires the Personalization Agent to use the Basic Access Control Authentication Mechanism or secure messaging.

OT.Prot_Abuse-Func (Protection against Abuse of Functionality) is ensured by the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other features which may not be used after TOE Delivery.

OT.Prot_Inf_Leak (Protection against Information Leakage) requires the TOE to protect confidential TSF data stored and/or processed in the MRTD’s chip against disclosure

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines, which is addressed by the SFR FPT_EMSEC.1,
- by forcing a malfunction of the TOE, which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE, which is addressed by the SFR FPT_PHP.3.

OT.Prot_Phys-Tamper (Protection against Physical Tampering) is covered by the SFR FPT_PHP.3.

OT.Prot_Malfunction (Protection against Malfunctions) is covered by (i) the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and (ii) the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

OT.AA_Proof (Proof of MRTD's chip authenticity by Active Authentication) is ensured by the Active Authentication Protocol provided by FIA_API.1 enforcing the identification and authentication of the MRTD's chip. The Active Authentication protocol requires FCS_RNG.1 (for the generation of the challenge), and FCS_COP.1/SHA (for the host challenge hashing) and FCS_COP.1/SIG_GEN (for the signature generation). The Active Authentication private Key is used. This TOE secret data is created during Personalization (Phase 3) according to FCS_CKM.1/KP (for Key generation mechanism), and by authorized agent as required by FMT_MTD.1/ AAPK.

6. TOE summary specification (ASE_TSS)

This set of TSFs manages the identification and/or authentication of the external user and enforces role separation (FMT_SMR.1).

6.1 SF.Access Control

This function checks that for each operation initiated by a user, the security attributes for user authorization (FMT_SMR.1) and data communication required are satisfied.

Control over the Terminal gaining access to MRTD's chip data (FDP_ACC.1, FDP_ACF.1) based on authentication status of the Terminal and Terminal authorizations

Control over the authorization of Manufacturer during Pre-personalization Phase 2 to:

- Write the initialization data and pre-personalization data (FMT_MTD.1/INI_ENA)

Control over the authorization of Personalization Agent during Personalization Phase 3 to:

- Write and Read EF.COM, EF.SOD, EF.DG1 to EF.DG16 (FDP_ACF.1.2 (1))
- Create and import initial Active Authentication Private Key (FMT_MTD.1/AAPK)
- Write Document Basic Access Keys (FMT_MTD.1/KEY_WRITE)
- Disable read access to initialization data for users (FMT_MTD.1/INI_DIS)

Control over the Basic Inspection System during Usage Phase 4 to:

- Read EF.COM, EF.SOD, EF.DG1, EF.DG2, EF.DG5 to EF.DG16 (FDP_ACF.1.2 (2))
- Prevent reading of EF.DG3 (fingerprint) and EF.DG4 (Iris) (FDP_ACF.1.4 (3))
- Create new Active Authentication Keys (FMT_MTD.1/AAPK)

Control over any non-authenticated Terminal during Usage Phase 4 to:

- Prevent modification of EF.DG1 to EF.DG16 (FDP_ACF.1.4 (1))
- Prevent reading of EF.DG1 to EF.DG16 (FDP_ACF.1.4 (2))
- Prevent reading Document Basic Access Keys, Personalization Agent Keys, Active Authentication Private Key (FMT_MTD.1/KEY_READ)

Control over the enforcement of Secure Messaging over:

- Importation and exportation of data (including but not restricted to EF.COM, EF.SOD, EF.DG1-EF.DG16) after successful BAC Authentication (FDP_UCT.1, FDP_UIT.1)

6.2 SF.Administration

In Initialization Phase (informative, covered by ALC family), this TSF provides Card initialization and pre-personalization services as per GlobalPlatform. This includes but is not restricted to card initialization, patch loading, applet installation and instantiation.

When the TOE is ready to be personalized, the Administrator will create the authentication data for the Personalization Phase within the Applet and terminate this manufacturing stage by disabling the card content loading and installation functions.

In Personalization Phase, the Administrator is identified through the relevant access rights (FMT_SMR.1) and performs administrative activities like initialization of the file system, configuration/personalization of the TOE. The key used for data protection is generated during the initialization of the file system (FCS_RNG.1).

In Usage phase, the Administrator is identified through the relevant access rights (FMT_SMR.1) and performs administrative activities.

6.3 SF.Active Authentication

Active Authentication is provided by this TSF based on the availability of DG15 in the MRTD's chip information data (FIA_API.1). This is decided by the Personalization Agent during phase 3 when the LDS is personalized. The Terminal is then allowed to select this authentication key and proceed with Active Authentication after successful BAC Authentication (to prevent the privacy threat Challenge Semantics). See the inspection procedures in section 2.4 of [10].

This TSF involves an optional asymmetric Key Pair (KPr_{AA}, KPu_{AA}) which public part is stored in DG15 and private part is stored securely within the chip. This Key Pair is securely generated on the TOE under request of the Personalization Agent (FCS_CKM.1/KP).

This TSF ensures that the chip has not been substituted, by means of a challenge-response protocol between the inspection system and the MRTD's chip. The TOE's challenge is a random generated by the TOE (FCS_RNG.1). And the challenge-response involves an RSA signature generation based on ISO/IEC 9796-2 Digital Signature scheme 1 respectively an ECC signature based on ECDSA as specified in ANSI X9.62 (FCS_COP.1/SIG_GEN, FCS_COP.1/SHA *SHA-256*). The use of challenges enforces a protection against replay (FIA_UAU.4).

IC power variation emanation is below state of the art values, and physical access to the authentication data is protected during this SF activity (FPT_EMSEC.1).

6.4 SF.BAC Authentication

This TSF provides the Basic Access Control passive authentication protocol (The Terminal is then allowed to select this authentication key and proceed with BAC Authentication (FIA_UAU.1, FIA_UID.1, and FIA_UAU.5). This is the only authentication mechanism that involves symmetric keys (KB_{Enc} and KB_{MAC}): TDES 112 bits (FCS_COP.1/AUTH).

As part of the protocol, the BAC Session Keys are derived from the MRZ of the MRTD's chip: this is done using SHA-1 (FCS_COP.1/SHA). The authentication initialization requires that the MRTD's chip generates 8 bytes challenge (nonce r_{PICC}) that is read by the Basic Inspection System (FIA_UAU.1), and 16 bytes Key (K_{PICC}) (FCS_RNG.1). The MRTD BAC authentication stages also require TDES encryption of 32 bytes of concatenated data and a Retail MAC computation over the 32 bytes of encryption output (FCS_COP.1/MAC). The Basic Inspection System also generated a pair (K_{PCD}, r_{PCD}). The use of challenges enforces a protection against replay (FIA_UAU.4).

Completion of the BAC Authentication protocol means that a Secure Messaging session is started with the session keys (K_{ENC} and K_{MAC}) derived from the derived according to [9] from the common master secret $K_{Master} = K_{PICC} \oplus K_{PCD}$ and a Send Sequence Counter SSC derived from r_{PICC} and r_{PCD} (FCS_CKM.1/BAC). All further communication with the TOE is handled by SF.Secure Messaging Security Function, enforcing confidentiality and integrity over transferred data (FIA_UAU.5).

In case the BAC authentication protocol fails (the TOE being unable to identify the Terminal as being a legitimate Basic Inspection System) the TOE records one authentication failure. If the Terminal reaches a pre-defined amount of successive authentication failures, the BAC Authentication Key is blocked (FIA_AFL.1).

6.5 SF.Personalizer Authentication

The Personalization Agent is authenticated by the TOE using its symmetric key (FIA_UAU.5). He is able to read the random identifier in that phase (FIA_UAU.1, FIA_UID.1).

The authentication requires a Challenge-response External Authentication using TDES (with key length of 112 bits) or AES (with key length of 128, 192, or 256 bits) (FCS_COP.1/ AUTH, FCS_RNG.1). The retry counter for the Personalization Agent key is set to "1" (FIA_AFL.1).

IC power variation emanation is below state of the art values, and physical access to the authentication data is protected during this SF activity (FPT_EMSEC.1).

6.6 SF.Secure Messaging

Commands and responses are exchanged between the TOE and the external device.

The SF.Secure_Messaging function is capable of providing a secure communication channel between legitimate end points both of the TOE and the external device. The secure communication channels are enforced by cryptographic functions.

This function is responsible for confidentiality (FDP_UCT.1) and data authentication/integrity (FDP_UIT.1). Confidentiality is ensured through the encryption of communication data by symmetric cryptography by the use 3DES operations (FCS_COP.1/ENC). Data authentication and integrity is achieved by calculating of a cryptographic checksum (MAC) (FCS_COP.1/MAC).

This function provides means to detect if modification, deletion, insertion or replay is occurring during a Secure Messaging session. In such cases, this TSF will terminate the session and securely destroy the session keys (FCS_CKM.6). A session is also terminated upon reset of the TOE. A re-authentication using the Chip Authentication protocol is required after termination of a Secure Messaging session (FIA_UAU.6). Encryption operations are protected against DPA/SPA, timing attacks, and electromagnetic emanation (FPT_EMSEC.1).

6.7 SF.Crypto

This Security Function is responsible for providing cryptographic support to all the other Security Functions including secure key generation and operations on data such as encrypt and sign:

- Secure generation of asymmetric RSA or ECC Key Pair (FCS_CKM.1/KP). Key generation is protected against SPA, Timing attacks, and electromagnetic emanation (FPT_EMSEC.1) and includes Key Pair Correspondence verification.
  - The random number generator of the IC is used by the TOE whenever the generation of a nonce is required (FCS_RNG.1).
  - Adequate number of Rabin Miller test rounds is performed in addition to GCD test in order to ensure correct generation of primes in case of RSA.

- Data hashing using SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FCS_COP.1/SHA)
- Digital signature generation with RSA Standard/CRT Key Pair of lengths 1024 to 4096 bits and ECC Key Pair of lengths 192 to 521 bits (FCS_COP.1/SIG_GEN),
- Digital signature verification (for Terminal Authentication) with RSA Standard/CRT Key Pair of lengths 1024 to 4096 bits and ECDSA Key Pair of lengths 192 to 521 bits (FCS_COP.1/SIG_VER),
- TDES 2 Keys and 3 Keys in CBC, ECB, R-MAC modes (FCS_COP.1/ENC, FCS_COP.1/MAC, FCS_COP.1/AUTH)
- BAC protocol related cryptography (FCS_CKM.1/BAC)
- Secure destruction of cryptographic key secret or private material (FCS_CKM.6).

This TSF enforces protection of Key material during cryptographic functions processing and Key Generation, against state-of-the-art attacks, including IC power consumption analysis (FPT_EMSEC.1)

6.8 SF.Secure Personalization Management

This TSF provides Card initialization and pre-personalization services (FMT_SMF.1) as per GlobalPlatform. This includes but is not restricted to card initialization, patch loading, applet installation and instantiation.

This TSF also provides MRTD's chip personalization functions to allow the Personalization Agent to create and set the initial MRTD's LDS data (FMT_SMF.1, FAU_SAS.1). This includes disabling read access to Initialization data at completion of the personalization phase (FMT_SMF.1).

6.9 SF.Protection

This Security Function is responsible for protection of the TSF data, user data, and TSF functionality. The SF. Protection function is composed of software implementations of test and security functions including:

- Performing self tests of the TOE at each power-up (FPT_TST.1)
- Deleting authentication resources (Biometric Data, PINs, secret and private keys) when relevant memory is de-allocated (FCS_CKM.6)
- Validating the integrity of all stored cryptographic keys and PINs before use and informing the Terminal when such validation fails (FPT_TST.1).
- Performing a set of test to verify that the underlying cryptographic algorithms are operating correctly (FPT_TST.1).
- Initializing memory after reset
- Initializing memory of de-allocated data
- Preserving secure state after sensitive processing failure (RNG, EEPROM handling) or potential physical tampering or intrusion detection (FPT_FLS.1, FPT_PHP.3)
- Ensuring that Information is not leaked (FPT_EMSEC.1).

The TOE provides the ability to patch some identified native functions of the original TOE. This mechanism is available during Initialization phase but in the case of this TOE, no patch is loaded.

This TSF prevents re-activation of de-activated or disabled or terminated mechanisms: the code area and data area are protected (FMT_LIM.1, FMT_LIM.2)

7. Additional Rationale

7.1 Dependencies Rationale

7.1.1 SFR Dependencies

Requirement	Dependencies
Functional Requirements	
FAU_SAS.1	No dependencies
FCS_CKM.1/ BAC	FCS_COP.1/MAC, FCS_COP.1/ENC, FCS_CKM.6, FCS_RNG.1
FCS_CKM.1/ KP	FCS_COP.1/SIG_GEN, FCS_CKM.6, FCS_RNG.1
FCS_CKM.6	FCS_CKM.1/BAC, FCS_CKM.1/KP
FCS_COP.1/ SHA	FCS_CKM.6, unsupported dependencies, see 7.1.3 for justification
FCS_COP.1/ ENC	FCS_CKM.1/BAC, FCS_CKM.1/KP, FCS_CKM.6, FCS_RNG.1
FCS_COP.1/ AUTH	FCS_RNG.1, unsupported dependencies, see 7.1.3 for justification
FCS_COP.1/ MAC	FCS_CKM.1/BAC, FCS_CKM.6, FCS_RNG.1
FCS_COP.1/ SIG_GEN	FCS_CKM.1/BAC, FCS_CKM.1/KP, FCS_CKM.6, FCS_RNG.1
FCS_RNG.1	No dependencies
FDP_ACC.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, unsupported dependencies, see 7.1.3 for justification
FDP_UCT.1	FDP_ACC.1, unsupported dependencies, see 7.1.3 for justification
FDP_UIT.1	FDP_ACC.1, unsupported dependencies, see 7.1.3 for justification
FIA_AFL.1	FIA_UAU.1
FIA_API.1	No dependencies
FIA_UAU.1	FIA_UID.1
FIA_UAU.4	No dependencies
FIA_UAU.5	No dependencies
FIA_UAU.6	No dependencies
FIA_UID.1	No dependencies
FMT_LIM.1	FMT_LIM.2
FMT_LIM.2	FMT_LIM.1
FMT_MTD.1/ AAPK	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/ INI_ENA	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/ INI_DIS	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/ KEY_WRITE	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/ KEY_READ	FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	No dependencies
FMT_SMR.1	FIA_UID.1

FPT_EMSEC.1	No dependencies
FPT_FLS.1	No dependencies
FPT_PHP.3	No dependencies
FPT_TST.1	No dependencies

Table 12. SFR Dependencies

7.1.2 SAR Dependencies

The functional and assurance requirements dependencies for the TOE are completely fulfilled.

Requirement	Dependencies
ADV_ARC.1	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	ADV_TDS.4, ADV_IMP.1
ADV_IMP.1	ADV_TDS.4, ALC_TAT.2
ADV_INT.2	ADV_IMP.1, ADV_TDS.4, ALC_TAT.2
ADV_TDS.4	ADV_FSP.5
AGD_OPE.1	ADV_FSP.5
AGD_PRE.1	No dependencies
ALC_CMC.4	ALC_CMS.5, ALC_DVS.2, ALC_LCD.1
ALC_CMS.5	No dependencies
ALC_DEL.1	No dependencies
ALC_DVS.2	No dependencies
ALC_LCD.1	No dependencies
ALC_TAT.2	ADV_IMP.1
ASE_CCL.1	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependencies
ASE_INT.1	No dependencies
ASE_OBJ.2	ASE_SPD.1
ASE_REQ.2	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependencies
ASE_TSS.1	ADV_FSP.5, ASE_INT.1, ASE_REQ.2
ATE_COV.2	ADV_FSP.5, ATE_FUN.1
ATE_DPT.3	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	ATE_COV.2
ATE_IND.2	ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.3	ADV_ARC.1, ADV_FSP.5, ADV_TDS.4, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1
ASE_COMP.1	No dependencies
ADV_COMP.1	No dependencies
ATE_COMP.1	No dependencies
AVA_COMP.1	No dependencies
ALC_COMP.1	No dependencies

Table 13. SAR Dependencies

7.1.3 Justification of Unsupported Dependencies

The security functional dependencies for the TOE are not completely supported:

FCS_COP.1/ SHA	The hash algorithm required by the SFR FCS_COP.1/SHA does not use any key material and is purely deterministic, therefore neither a key generation (FCS_CKM.1), random data (FCS_RNG.1) nor an import (FDP_ITC.1/2) is necessary.
FCS_COP.1/ AUTH	The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE lifecycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.6, too.
FDP_ACF.1	The access control TSF according to FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.
FDP_UCT.1	The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the MRTD and the GIS. There is no need for the SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.
FDP_UIT.1	

Table 14. Unsupported Dependencies

7.2 TOE Summary Specifications Rationale

7.2.1 Security Function Coverage

The following table covers the mapping between TOE Security Functional Requirement and TSF:

TOE SFRs / TOE Security Functions	SF.Acess Control	SF.Administration	SF.Active Auth	SF.BAC Auth	SF.Personailzer Authentication	SF.Secure Messaging	SF.Crypto	SF.Secure Personalization management	SF.Protection
FAU_SAS.1								x	
FCS_CKM.1/ BAC				x			x		
FCS_CKM.1/ KP			x				x		
FCS_CKM.6						x	x		x
FCS_COP.1/ SHA				x			x		
FCS_COP.1/ ENC						x	x		
FCS_COP.1/ AUTH				x	x		x		

FCS_COP.1/ MAC				x		x	x		
FCS_COP.1/ SIG_GEN			x				x		
FCS_RNG.1		x	x	x	x		x		
FDP_ACC.1	x								
FDP_ACF.1	x								
FDP_UCT.1	x					x			
FDP_UIT.1	x					x			
FIA_AFL.1				x	x				
FIA_API.1			x						
FIA_UAU.1				x	x	x		x	
FIA_UAU.4			x	x					
FIA_UAU.5				x	x	x			
FIA_UAU.6						x			
FIA_UID.1				x	x				
FMT_LIM.1									x
FMT_LIM.2									x
FMT_MTD.1/ AAPK	x								
FMT_MTD.1/ INI_ENA	x								
FMT_MTD.1/ INI_DIS	x								
FMT_MTD.1/ KEY_WRITE	x								
FMT_MTD.1/ KEY_READ	x								
FMT_SMF.1		x						x	
FMT_SMR.1	x	x	x	x	x				
FPT_EMSEC.1			x		x		x		x
FPT_FLS.1									x
FPT_PHP.3									x
FPT_TST.1									x

Table 15. TOE Security Requirements to Security Function Mapping

7.2.2 Rationale for assurance measures

Each assurance requirement is covered by an assurance measure.

Assurance Requirements / Assurance Measures	AM_ADV	AM_AGD	AM_ALC	AM_ATE	AM_AVA
ADV	x				
AGD		x			
ALC			x		
ATE				x	
AVA					x

Table 16. Mapping Assurance Requirements to Assurance Measures

7.3 Rationale for Extensions

Extensions are based on the Protection Profile [8] and have all been adopted by the developer of the TOE, however in accordance with the CC:2022 Transition Policy [24], SFRs introduced in CC:2022 Part 2 [2] replace those defined in the PP. See Table 3: PP Extended Component Definitions, such that only FAU_SAS.1 is taken from the PP.

7.4 PP Claim Rationale

This ST includes all the security objectives and requirements claimed by PP [7] and all of the operations applied to the SFRs are in accordance with the requirements of this PP.

7.4.1 SPD Rationale

All the assets, assumptions, threats and OSPs of each claimed PPs have been strictly applied to this TOE.

The following threats have been added:

T.Counterfeit has been added as the TOE may support the Active Authentication Protocol. This mechanism prevents a threat the MRTD's chip is counterfeit.

The following assumptions have also been added:

A.Pers_Agent_AA assumption has been added as the TOE personalization phase may include personalization of the Active Authentication (AA) Keys.

A.Insp_Sys_AA assumption has been added as the Inspection system should proceed to Active Authentication if the corresponding Keys are present on the MRTD's chip (Public Key present in EF.DG15).

7.4.2 Objectives Rationale

The following objectives for the TOE have been added to those of the PP [8]:

OT.AA_Proof objective has been added to cover the fact that the card may support Active Authentication (AA) and provide a secure mean to the inspection system to authenticate the TOE as a genuine MRTD's chip.

The following objectives for the TOE environment have been added to those of the PP [7]:

OE.Exam_MRTD_AA objective has been added to cover the fact that the card may support Active Authentication (AA) and the inspection system should always examine the MRTD passport book and perform AA when provided.

OE.Active_Auth_Key objective has been added to cover the fact that the card may support Active Authentication (AA) and the inspection system should always handle the AA Key in a secure manner: that key is generated in the TOE and the public part should be written in EF.FG15.

7.4.3 SFR Rationale

The selections and assignments performed in the TOE are compliant with PP [7].

Selections and refinements of SFRs allowable by PP [7] were performed and are noted by using *underline italic* text. The following SFRs from the PPs have been reworked.

Assignments:

- FCS_CKM.6
- FCS_RNG.1
- FIA_AFL.1
- FPT_EMSEC.1
- FPT_TST.1

Selections:

- FCS_COP.1/ SHA
- FCS_COP.1/ AUTH
- FIA_UAU.4
- FIA_UAU.5
- FPT_TST.1

Due to the introduction of Active Authentication (AA), some SFRs have been modified:

- FCS_CKM.1 has been renamed FCS_CKM.1/ BAC (for Basic Access Control)
- FIA_UAU.4 has been modified to also cover the AA protocol
- FMT_MTD.1/ KEY_READ has been modify to also prevent AA Private Key read
- FPT_EMSEC.1 has been modified to also protect the AA Private Key

7.4.4 PP Additions

Some SFRs have been added to the set of SFRs proposed by PP [7].

The following SFRs have been added in relation to the addition of Active Authentication:

- FCS_CKM.1/KP: AA Key Pair generation
- FCS_COP.1/SIG_GEN: Data Signature Generation using the AA Private Key
- FIA_API.1: Active Authentication Protocol
- FMT_MTD.1/AAPK: AA Keys access control

7.4.5 PP compliancy

The TOE type is compliant with the claimed PP: the TOE is an ICAO MRTD's chip providing all means of identification and authentication of the TOE itself, the MRTD's traveler and possibly the Terminal.

The TOE is compliant with the representation provided in the ICAO Machine Readable Travel Document Chip with Basic Access Control PP [9].

The compliance is strict: the addition of specific TOE security mechanisms to the security principles of this Security Target required only the addition of one Threat and three TOE Objectives.

These additions do not affect the concept defined in the PP [7] and this ST is a suitable solution to the generic security problem described in the PP.

8. Terminology

Term	Definition
Active Authentication	Security mechanism defined in [9] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State of Organization.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization.
Basic Access Control (BAC)	Security mechanism defined in [9] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical MRTD.
Biographical data (biodata)	The personalized details of the MRTD holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [9]
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Certificate chain	Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [9]
Country Signing CA Certificate (CCSCA)	Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority stored in the inspection system.
Country Verifying Certification Authority	The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing State or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD.

Term	Definition
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [9], normative appendix 5, A5.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
Document Basic Access Keys	Pair of symmetric (two-key) TDES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system [9]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SOD)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [9]
Document Verifier	Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations.
Eavesdropper	A threat agent with Enhanced-Basic attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [9]
Extended Access Control	Security mechanism identified in [9] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate itself with Personalization Agent Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System	A General Inspection System which (i) implements the Chip Authentication Mechanism, (ii) implements the Terminal Authentication Protocol and (iii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

Term	Definition
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [9]
General Inspection System	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [9]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person’s document. [9]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else’s travel document or visa; or (d) no travel document or visa, if required. [9]
Initialization	Process of writing Initialization Data (see below) to the TOE (cf.1.3.6.2, TOE lifecycle phase 2 step 3).
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD’s material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [9]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.

Term	Definition
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization.
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [9]
Issuing State	The Country issuing the MRTD. [9]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [9]. The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [9] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) a. personal data of the MRTD holder b. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), c. the digitized portraits (EF.DG2), d. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and e. the other data according to LDS (EF.DG5 to EF.DG16) f. EF.COM and EF.SOD
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
Machine readable travel document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [9]
Machine readable visa (MRV)	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [9]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [9]

Term	Definition
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [9]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes - the file structure implementing the LDS [9], - the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO.
MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object
Personalization	The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment" (cf. 1.3.6.3, TOE lifecycle phase 3 step 6).
Personalization Agent	The agent acting on the behalf of the issuing State or Organization to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.

Term	Definition
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Key	Symmetric cryptographic authentication key used (i) by the Personalization Agent to prove his identity and to get access to the logical MRTD and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6.
Physical travel Document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and (4) other data
Pre-Personalization	Process of writing Pre-Personalization Data (see below) to the TOE including the creation of the MRTD Application (cf.1.3.6.2, TOE lifecycle phase 2 step 5)
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between lifecycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with a unique identifier and a unique asymmetric Active Authentication Key Pair of the chip.
Receiving State	The Country to which the Traveler is applying for entry. [9]
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [9]
Secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 Skimming Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
Travel document	A passport or other official document of identity issued by a State or Organization which may be used by the rightful holder for international travel.
Traveler	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

Term	Definition
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
Un-personalized MRTD	The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalization Agent from the Manufacturer.
User data	Data created by and for the user that does not affect the operation of the TSF.
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [9]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

9. References

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 2022, Revision 1, Nov 2022. CCMB-2022-011-001

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 2022, Revision 1, Nov 2022. CCMB-2022-011-002

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 2022, Revision 1, November 2022. CCMB-2022-011-003

[4] Common Methodology for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, Version 2022, Revision 1, November 2022. CCMB-2022-011-004

[5] Common Methodology for Information Technology Security Evaluation, Part 5: Pre-Defined packages of security requirements, Version 2022, Revision 1, November 2022. CCMB-2022-011-005

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Version 2022, Revision 1, November 2022. CCMB-2022-011-006

[7] BSI-CC-PP0055 – Protection Profile - Machine Readable Travel Document with “ICAO Application”, Basic Access Control – EAL 4+ – Version: 1.10, 25th March 2009

[8] BSI-CC-PP0056-V2-2012 – Protection Profile - Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE (EAC PP) – EAL 4+ – Version: 1.3.0, 20th January 2012

[9] ICAO Doc 9303, Machine Readable Travel Documents, Seventh Edition, 2015, International Civil Aviation Organization

[10] Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26 February 2015.

[11] ISO/IEC 9796-2: Information technology — Security techniques — Signature Schemes giving message recovery — Part 2: Integer factorization based mechanisms, 2002

[12] FIPS PUB 180-2, FIPS Publication – Secure hash standard (+ Change Notice to include SHA-224), 2002, NIST

[13] FIPS PUB 46-3, FIPS Publication – Data Encryption Standard (DES), Reaffirmed 1999 October 25, U.S. Department of Commerce/NIST

[14] IEEE 1363-2000 – IEEE Standard Specification for Public-Key Cryptography

[15] PKCS#1: RSA Cryptography Standard, Version 1.5

[16] NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3), Security Target Lite, NXP Semiconductors, Revision 2.0, 4 August 2025

[17] JCOP 4.5 P71 Security Target Lite for JCOP 4.5 P71, NXP Semiconductors, Rev. 2.9, 05 September 2025

[18] ChipDoc 4.2 Applet User Guide Manual, Ref. 654218, Revision 1.8, Date: 27 April 2026

[19] ChipDoc 4.2 Applet ICAO Personalization Guide, Ref. 654315, Revision: 1.5, Date: 27 April 2026

[20] GlobalPlatform Technology - Secure Element Management Service, CSv2.3 Amendment I, ref GPC_SPE_121, v1.1

[21] ANSI X9.62-2005: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute (ANSI), 2005.

[22] ChipDoc 4.2 Applet Release Note – Release Note for ChipDoc 4.2.0.4JxR Applet, Rev. 1.0, 16 January 2026.

[23] FIPS PUB 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/National Institute of Standards and Technology, 26 November 2001.

[24] Common Criteria Recognition Arrangement, Management Committee, Policies and Procedures: Transition Policy to CC:2022 and CEM:2022, CCMC-2023-04-001, 20 April 2023

[25] Bundesamt fuer Sicherheit in der Informationstechnik. AIS20/31: A proposal for: Functionality classes for random number generators, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.1, 2. December 2011

[26] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), CCMB-2024-02-v1_1, July 2024

10. Legal information

10.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

10.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors accepts no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications. In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — While NXP Semiconductors has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer's applications and products, and NXP Semiconductors accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

10.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

11. List of figures

Fig 1. Components of the TOE 3
Fig 2. TOE LifeCycle.....10

12. List of tables

Table 1. ST Reference and TOE Reference 3
Table 2. Reference to Certified Micro Controller with IC Dedicated Software and Crypto Library 7
Table 3. Reference to certified Platform 8
Table 4. Delivery Items 12
Table 5. PP0055 Extended Components in CC:2022 ... 16
Table 6. PP0056 Extended Components in CC:2022 ... 16
Table 7. Security Environment to Security Objectives Mapping 31
Table 8. PP Extended Component Definitions 34
Table 9. Assurance Requirements: EAL 4 augmented . 51
Table 10. Assurance Components of COMP Package ... 51
Table 11. Functional Requirement to TOE Security Objective Mapping 54
Table 12. SFR Dependencies 64
Table 13. SAR Dependencies 64
Table 14. Unsupported Dependencies 65
Table 15. TOE Security Requirements to Security Function Mapping 66
Table 16. Mapping Assurance Requirements to Assurance Measures 66

13. Contents

1. ST Introduction (ASE_INT) 3
1.1 ST Reference and TOE Reference 3
1.2 TOE Overview 3
1.2.1 TOE usage and security features for operational use 4
1.3 TOE Description 5
1.3.1 General 5
1.3.2 MRTD's chip 5
1.3.3 Basic Access Control 6
1.3.4 Active Authentication 6
1.3.5 TOE Components and Composite Certification 7
1.3.5.1 Micro Controller 7
1.3.5.2 Security IC Dedicated Software 7
1.3.5.3 Security IC Embedded Software 8
1.3.6 TOE Lifecycle 8
1.3.6.1 Phase 1 "Development" 8
1.3.6.2 Phase 2 "Manufacturing" 9
1.3.6.3 Phase 3 "Personalization of the MRTD" 11
1.3.6.4 Phase 4 "Operational Use" 11
1.3.7 TOE Identification 12
1.3.7.1 TOE Delivery 12
1.3.7.2 Identification of the TOE 12
1.3.8 Evaluated Package Types 12
2. Conformance Claims (ASE_CCL) 14
2.1 CC Conformance Claim 14
2.2 Package Claim 14
2.3 PP Claim 15
2.4 Rationale Regarding CC:2022 15
3. Security Problem Definition (ASE_SPD) 17
3.1 Assets 17
3.2 Subjects 18
3.3 Assumptions 19
3.4 Threat agent 21
3.5 Threats 21
3.6 Organisational Security Policies 24
4. Security Objectives (ASE_OBJ) 25
4.1 SOs for the TOE 25
4.2 SOs for the Environment 28
4.2.1 Issuing State or Organization 28
4.2.2 Receiving State or Organization 29
4.3 Security objectives rationale 30
4.3.1 Security Objectives Coverage 30
4.3.2 Security Objectives Sufficiency 31
4.3.2.1 Policies and Security Objective Sufficiency 31
4.3.2.2 Threats and Security Objective Sufficiency 31
4.3.2.3 Assumptions and Security Objective Sufficiency 32
5. Extended Components Definition (ASE_ECD) 34
5.1 Audit data storage (FAU_SAS) 34
5.2 Security Requirements (ASE_REQ) 36
5.3 TOE Security Functional Requirements 38
5.3.1 Security Audit (FAU) 38
5.3.1.1 Audit Storage (FAU_SAS.1) 38
5.3.2 Cryptographic support (FCS) 38
5.3.2.1 Cryptographic key generation (FCS_CKM.1) 38
5.3.2.2 Cryptographic key destruction (FCS_CKM.6) 39
5.3.2.3 Cryptographic operation (FCS_COP.1) 39
5.3.2.4 Random Number Generation (FCS_RNG.1) 40
5.3.3 User data protection (FDP) 42
5.3.3.1 Subset access control (FDP_ACC.1) 42
5.3.3.2 Security attribute based access control (FDP_ACF.1) 42
5.3.3.3 Basic data exchange confidentiality (FDP_UCT.1) 42
5.3.3.4 Data exchange integrity (FDP_UIT.1) 43
5.3.4 Identification and authentication (FIA) 43
5.3.4.1 Authentication Failure handling (FIA_AFL.1) 43
5.3.4.2 Authentication Proof of Identity (FIA_API.1) 44
5.3.4.3 Timing of authentication (FIA_UAU.1) 44
5.3.4.4 Single-use authentication mechanisms (FIA_UAU.4) 44
5.3.4.5 Multiple authentication mechanisms (FIA_UAU.5) 45

For more information, visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 14 May 2026
Document identifier:CDv4.2_210311_ST_ICAO_BAC

5.3.4.6 Re-authenticating (FIA_UAU.6) 45
5.3.4.7 Timing of identification (FIA_UID.1) 46
5.3.5 Security management (FMT) 46
5.3.5.1 Limited capabilities (FMT_LIM.1) 46
5.3.5.2 Limited availability (FMT_LIM.2) 47
5.3.5.3 Management of TSF data (FMT_MTD.1) 47
5.3.5.4 Specifications of Management Functions (FMT_SMF.1) 48
5.3.5.5 Security roles (FMT_SMR.1) 48
5.3.6 Protection of the TSF (FPT) 48
5.3.6.1 TOE Emanation (FPT_EMS.1) 48
5.3.6.2 Failure with preservation of secure state (FPT_FLS.1) 49
5.3.6.3 Resistance to physical attack (FPT_PHP.3) 49
5.3.6.4 TSF testing (FPT_TST.1) 50
5.4 TOE Security Assurance Requirements 50
5.4.1 SARs Measures 50
5.4.2 SARs Rationale 51
5.5 Security Requirements Rationale 53
5.5.1 Security Requirement Coverage 53
5.5.2 Security Requirements Sufficiency 54
5.5.2.1 TOE Security Requirements Sufficiency 54
6. TOE summary specification (ASE_TSS) 58
6.1 SF.Access Control 58
6.2 SF.Administration 58
6.3 SF.Active Authentication 59
6.4 SF.BAC Authentication 59
6.5 SF.Personalizer Authentication 60
6.6 SF.Secure Messaging 60
6.7 SF.Crypto 60
6.8 SF.Secure Personalization Management 61
6.9 SF.Protection 61
7. Additional Rationale 63
7.1 Dependencies Rationale 63
7.1.1 SFR Dependencies 63
7.1.2 SAR Dependencies 64
7.1.3 Justification of Unsupported Dependencies 64
7.2 TOE Summary Specifications Rationale 65
7.2.1 Security Function Coverage 65
7.2.2 Rationale for assurance measures 66
7.3 Rationale for Extensions 66
7.4 PP Claim Rationale 67
7.4.1 SPD Rationale 67
7.4.2 Objectives Rationale 67
7.4.3 SFR Rationale 67
7.4.4 PP Additions 68
7.4.5 PP compliancy 68
8. Terminology 69
9. References 76
10. Legal information 78
10.1 Definitions 78
10.2 Disclaimers 78
10.3 Trademarks 78
11. List of figures 79
12. List of tables 80
13. Contents 81

For more information, visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 14 May 2026
Document identifier:CDv4.2_210311_ST_ICAO_BAC