NXP SmartePP_P71 - ICAO BAC with optional Active Authentication

Security Target Lite

Rev. 1.3 — 2 March 2021 Product evaluation document
NSCIB-20-0108259

Document information

Information	Content
Keywords	Security Target, ICAO, Basic Access Control (BAC)
Abstract	Security Target for NXP Smart ePP Product on NXP P71 Certified Hardware, implementing an ICAO ePP with Basic Access Control with Optional Active Authentication

Revision History

Revision history

Revision number	Date	Description
1.0	2020-12-11	Release Version
1.1	2021-01-08	Update Table 1 for 'lite' version
1.2	2021-02-26	Correct UGM reference in Table 3
1.3	2021-03-02	Update Platform Reference

1 Introduction

1.1 ST Reference and TOE Reference

Table 1. ST References

Title	Security Target Lite NXP SmartePP on P71 - BAC
ST Version	1.3
ST Date	2 March 2021
TOE Name	NXP SmartePP on P71
TOE Short Name	NXP SmartePP (P71)
TOE Version	03 00 00 10
Product Type	electronic Passport
CC Version	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 5, April 2017 (Part 1 [2], Part 2 [3] and Part 3 [4])
Protection Profile	Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control (BAC PP), certified under the reference BSI-CC-PP-0055-2009, Version 1.10, BSI-CC-PP-0055 [7].
Assurance Level	EAL 4+ (Augmented on ALC_DVS.2 - 'Sufficiency of Security Measures' and ALC_FLR.1 'Basic Flaw Remediation)

1.2 TOE Overview

The protection profile PP0055 [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) Doc 9303 [8]. 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.

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

1.2.1 TOE Usage and Operational Security Features

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:

- Visual (eye readable) biographical data and portrait of the holder,
- A separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and
- Data elements on the MRTD’s chip according to LDS for contactless machine reading

The authentication of the traveler is based on:

- The possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and
- Optional biometrics using the reference data stored in the MRTD.

The receiving State trusts a genuine MRTD of an issuing State or Organization.

For this Security Target 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 [6] 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 optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both1
   d. The other data according to LDS (EF.DG5 to EF.DG16) and
   e. The Document security object.

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) [8]. 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 to the logical MRTD and the Data Encryption of additional sensitive biometrics) as optional security measure in ICAO Doc9303, Machine Readable Travel Documents, 7th Edition, 2015 [8]. 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:

1. in integrity by write only-once access control and by physical means, and
2. in confidentiality by the BAC Mechanism.

This TOE addresses Active Authentication as an optional security mechanism but does not address EAC (Extended Access Control).

1.3 TOE Description

The Target of Evaluation (TOE) is the integrated circuit chip of the machine readable travel document (MRTD chip), loaded with a the native Card Operating System, SmartePP, programmed with the Logical Data Structure (LDS) providing Basic Access Control (BAC) and optionally Active Authentication defined by ICAO Doc 9303 [8].

The TOE comprises at least:

- the circuitry of the MRTD's chip [11]

- the IC Dedicated Software and Crypto Library [11]
- the IC Embedded Software (smart ePP)
- a personalised filesystem, created in accordance with the guidance given
- the associated guidance documentation

1.3.1 TOE Form Factor and Interfaces

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 end products embedding the TOE:

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

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 evaluation in other TOEs.

1.3.2 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:

1. Optically reads the MRTD
2. 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 [8], normative appendix 5.

1.3.3 Active Authentication

This TOE offers an optional mechanism called Active Authentication, specified in ICAO Doc 9303 [8]. This security feature is a digital security feature that prevents cloning by introducing a key pair, unique to each chip:

- The public key is stored in data group DG15 and thus protected by Passive Authentication.
- The corresponding private key is stored in secure memory and may only be used internally by the MRTD chip and cannot be read out.

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.

1.3.4 TOE Components and Composite Certification

The TOE is a composite product with the underlying Security IC being an NXP Flash based Secure Microcontroller N7121 [11] certified along with the embedded Security firmware and Cryptographic Libraries in accordance with BSI to EAL 6+.

Table 2. TOE Composition

Title	NXP SmartePP on P71
Platform	NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2)
Platform Certificate	BSI-DSZ-CC-1136-2021
Assurance Level	EAL 6+ (ALC_FLR.1, ASE_TSS.2)

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

1.3.5 TOE Lifecycle

The TOE Lifecycle is fully described in the composite product Protection Profile [7], with reference to the BSI-CC-PP0035-2007, which has been superceded by PP0084[6]. This security target defines the composite product in terms of the lifecycle definitions given in the latter PP0084 to align with the N7121 Security Target[11].

The IC Developer, IC Manufacturer and the Embedded Software Developer of this TOE is NXP Semiconductors. In particular the software development for this composite TOE takes place at NXP sites in San Jose and Glasgow.

All other sites contributing to the Lifecycle of this TOE can be read from the certification report of the underlying IC.

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.

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 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.

(Step 5 - PrePersonalisation)

During the step Pre-Perso, the MRTD manufacturer

1. creates the MRTD application and
2. equips MRTD's chips with pre-personalization Data.

IC Pre-Personalization

To create the application, it is necessary to create an MRTD file system. For e-passport products, 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. 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.

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 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.

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.

1.3.6 TOE Delivery

The TOE delivery comprises the following items:

Table 3. TOE Delivery Items

Type	Name	Version	Form
Product	NXP SmartePP on P71	03 00 00 10	NXP Secure Smart Card Controller N712 including on-chip security software and Crypto Library and the SmartePP application
Document	SmartePP User manual and administrator guide	[9]	DocStore Document
Document	SmartePP ICAO Personalization Guide	[10]	DocStore Document

1.3.7 TOE Identification

The TOE identity may be confirmed by retrieving the tags listed in using a GET DATA command as described in the SmartePP UGM [9], section 2.1

Table 4. TOE References

Title	NXP SmartePP on P71
Embedded Name (Tag 0x0100)	53 6D 61 72 74 65 50 50 "SmartePP"
Embedded Version (Tag 0x0116)	03 00 00 10

1.3.8 TOE 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, 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 appropriate to their needs.

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target claims strict conformance to the Common Criteria version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001, April 2017 [2].
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017 [3].
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017 [4].

For the evaluation the following methodology will be used:

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

Extensions based on the Protection Profile are reused

- FAU_SAS.1 ‘Audit data storage’
- FCS_RND.1 ‘Generation of random numbers’
- FMT_LIM.1 ‘Limited capabilities’
- FMT_LIM.2 ‘Limited availability’
- FPT_EMSEC.1 ‘TOE emanation’

A further extension FIA_API - 'Authentication Proof of Identity' is defined in Section 5.1 in order to address the optional addition of Active Authentication.

2.2 PP Conformance Claim

This Security Target claims strict conformance to the ICAO Protection Profile; Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control (BAC PP), certified under the reference BSI-CC-PP-0055-2009, Version 1.10, BSI-CC-PP-0055 [7].

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 have been added to the related sections of this Security Target. The additional Security Objectives for the toe are listed in Table 13 and the associated SFRs are listed in Table 20 with a rationale given.

2.3 Package Claim

The assurance level for the TOE is CC EAL 4 augmented with ALC_DVS.2 'sufficiency of security measures' and ALC_FLR.1 'Basic Flaw Remediation'

3 Security Problem Definition

3.1 SPD Introduction

The Security Problem definition of the Protection Profile, PP0055 [7] apply entirely to this Security Target.

3.1.1 Assets

The Assets described in section 3.1 of the Protection Profile, BSI-CC-PP0055 [7] entirely apply to this Security Target and are listed in Table 5 .

Table 5. Assets defined in the Protection Profile

Name
Logical MRTD Data
Authenticity of the MRTD's chip

3.1.2 Subjects

The Subjects described in section 3.1 of the Protection Profile, BSI-CC-PP0055 [7] entirely apply to this Security Target and are listed in Table 6.

Table 6. Subjects defined in the Protection Profile

Subjects
Manufacturer
Personalization Agent
Terminal
Inspection system (IS)
MRTD Holder
Traveler
Attacker

3.2 Assumptions

The Assumptions described in section 3.2 of the Protection Profile, BSI-CC-PP0055 [7] entirely apply to this Security Target and are listed in Table 7.

Table 7. Standard Assumptions defined in the Protection Profile

Name	Title
A.MRTD_Manufact	MRTD manufacturing on steps 4 to 6
A.MRTD_Delivery	MRTD delivery during steps 4 to 6
A.Pers_Agent	Personalization of the MRTD's chip
A.Insp_Sys	Inspection Systems for global interoperability
A.BAC-Keys	Cryptographic quality of Basic Access Control Keys

Table 8. Assumptions added to this Security Target

Name	Title
A.Pers_Agent_AA	Personalization of the MRTD's chip including Active Authentication
A.Insp_Sys_AA	Inspection Systems for global interoperability with Active Authentication

The assumptions added to the Security Target are defined below:

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_AA **Inspection Systems for global interoperability with Active Authentication**

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

3.3 Threats

The Threats described in section 3.3 of the Protection Profile, BSI-CC-PP0055 [7] entirely apply to this Security Target. They are listed in Table 9.

Table 9. Standard Threats against the TOE defined in the Protection Profile

Name	Title
T.Chip_ID	Identification of MRTD's chip
T.Skimming	Skimming the logical MRTD
T.Eavesdropping	Eavesdropping the communication between TOE and Inspection System
T.Forgery	Forgery of data on MRTD's chip
T.Abuse-Func	Abuse of Functionality
T.Information_Leakage	Information Leakage from MRTD's chip
T.Phys-Tamper	Physical Tampering
T.Malfunction	Malfunction due to Environmental Stress

Table 10. Threats added in this Security Target

Name	Title
T.Counterfeit	Counterfeit MRTD

The threat in Table 10 is defined below.

T.Counterfeit	**Counterfeit MRTD**
Adverse action:	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.
Threat agent:	The attacker in possession of one or more legitimate MRTDs
Asset:	Threatened asset is authenticity of logical MRTD data.

3.4 Organisational Security Policies

The Organisation Security Policies described in section 3.4 of the Protection Profile, BSI-CC-PP0055 [7] entirely apply to this Security Target.

Table 11. Standard OSPs defined in the Protection Profile

Name	Title
P.Manufact	Manufacturing of the MRTD's chip
P.Personalization	Personalization of the MRTD by issuing State or Organization only
P.Personal_Data	Personal data Protection Policy

3.5 Security Problem 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).

4 Security Objectives

4.1 Security Objectives for the TOE

The Security Objectives detailed in Section 4.1 of the Protection Profile, BSI-CC-PP0055 [7] entirely apply to this Security Target. They are listed in Table 12.

Additional Security Objectives are defined in Section 4.1.2 and listed in Table 13.

4.1.1 Standard Security Objectives for the TOE

Table 12. Standard Security objectives for the TOE defined in the Protection Profile

Name	Title
OT.AC_Pers	Access Control for Personalization of logical MRTD
OT.Data_Int	Integrity of Personal DAta
OT.Data_Conf	Confidentiality of personal data
OT.Identification	Identification and Authentication of the TOE
OT.Prot_Abuse-Func	Protection against Protection against Abuse of Functionality
OT.Prot_Inf_Leak	Protection against Information Leakage
OT.Prot_Phys-Tamper	Protection against Physical Tampering
OT.Prot_Malfunction	Protection against Malfunctions

4.1.2 Additional Security Objectives for the TOE

Table 13. Additional Security objectives for the TOE

Name	Title
OT.AA_Proof	Proof of MRTD’s chip authenticity by Active Authentication

4.1.2.1 OT.AA_Proof

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 ICAO Doc 9303 [8]

4.2 Security Objectives for the Operational Environment

The Security Objectives detailed in Section 4.2 of the Protection Profile[7] apply entirely to this Security Target.

4.2.1 Standard Security Objectives for the Operational Environment

Table 14. Standard Security objectives for the Operational Environment defined in the Protection Profile

Name	Title
OE.MRTD_Manufact	Protection of the MRTD Manufacturing
OE.MRTD_Delivery	Protection of the MRTD Delivery
OE.Personalization	Personalization of logical MRTD
OE.Pass_Auth_Sign	Authentication of logical MRTD by Signature
OE.BAC-Keys	Cryptographic quality of Basic Access Control Keys
OE.Exam_MRTD	Examination of the MRTD passport book
OE.Passive_Auth_Verif	Verification by Passive Authentication
OT.Prot_Logical_MRTD	Protection of data from the logical MRTD

4.2.2 Additional Security Objectives for the Operational Environment

This Security Target adds the security objectives for the operational environment listed in Table 15.

Table 15. Additional Security objectives for the Operational Environment

Name	Title
OE.Exam_MRTD_AA	Examination of the MRTD passport book using Active Authentication
OE.Active_Auth_Key	Active Authentication Key

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

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, defined in ICAO Doc 9303 [8] to verify the authenticity of the presented MRTD's chip.

4.3 Security Objectives Rationale

This rationale is available in the full version of the Security Target, available in certain cases only under NDA.

The rationale for the Security Objectives provided in Section 4.3 of the Protection Profile [7] apply entirely to this Security Target.

The added threat **T.Counterfeit "MRTD's chip"** addresses the threat 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
- OT.Prot_Malfunction

In addition, when the MRTD supports Active Authentication, the TOE provides 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.

The additional objectives for the TOE when Active Authentication is supported :

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:

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.DG15.

4.3.1 Security Objectives Sufficiency

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_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.

5 Extended Components

The underlying Protection Profile, BSI-CC-PP0055 [7], defines extended components in Section 5.

Table 16. Extended Components Defined by the Protection Profile

SFR	Title
FAU_SAS	Audit Data Storage
FCS_RNG	Generation of Random Numbers
FMT_LIM	Limited capabilities and availability
FPT_EMSEC	TOE Emanation

This Security Target defines the following additional Security Family

Table 17. Extended Components Defined for this Security Target

SFR	Title
FIA_API	Authentication Proof of Identity

5.1 Authentication Proof of Identity (FIA_API)

Family Behaviour

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component levelling

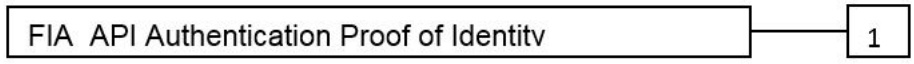

Figure 1. Component Levelling FIA_API

Management:

The following actions could be considered for the management functions in FMT:

- Management of authentication information used to prove the claimed identity.

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1	**Authentication Proof of Identity**
Hierarchical to:	No other components
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or role].

6 Security Requirements

This Security Target maintains a complete consistency with the description of the CC operations given in Section 6 of the PP.

This Security Target uses the security attribute definitions in exactly the manner described in Section 6 of the PP.

6.1 Security Functional Requirements for the TOE

This security functional requirements defined by Section 6.1 of the Protection Profile , PP0055 [7], apply entirely to this Security Target. The complete list of SFRs detailed in the Protection Profile are listed in Table 18, with an indication as to whether they have been modified via the permitted operations or not. The SFRs which are modified through the specified operations are listed in Table 19 and elaborated in subsequent subsections.

SFRs which have been introduced to this Security target to support Active Authentication are described in Section 6.1.3 and listed in Table 20.

6.1.1 SFRs from the Protection Profile

Table 18. Security Functional Requirements from the Protection Profile

SFR	Title	Modified
FAU_SAS.1	Audit Storage	No
FCS_CKM.1	Cryptographic key generation – Generation of Document Basic Access Keys by the TOE	No
FCS_CKM.4	Cryptographic key destruction - MRTD	Yes
FCS_COP.1/SHA	Cryptographic operation – Hash for Key Derivation	Yes
FCS_COP.1/ENC	Cryptographic operation – Encryption / Decryption Triple DES	No
FCS_COP.1/AUTH	Cryptographic operation – Authentication	Yes
FCS_COP.1/MAC	Cryptographic operation – Retail MAC	No
FCS_RND.1	Quality metric for random numbers	Yes
FIA_UID.1	Timing of identification	No
FIA_UAU.1	Timing of authentication	No
FIA_UAU.4	Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE	Yes
FIA_UAU.5	Multiple authentication mechanisms	Yes
FIA_UAU.6	Re-authenticating – Re-authenticating of Terminal by the TOE	No
FIA_AFL1	Authentication failure handling	Yes
FIA_ACC.1	Subset access control – Basic Access control	No
FIA_ACF.1	Basic Security attribute based access control – Basic Access Control	No
FIA_UCT.1	Basic data exchange confidentiality - MRTD	No
FDP_UIT.1	Data exchange integrity - MRTD	No
FMT_SMF.1	Specification of Management Functions	No
FMT_SMR.1	Security roles	No

SFR	Title	Modified
FMT_LIM.1	Limited capabilities	No
FMT_LIM.2	Limited availability	No
FMT_MTD.1/INI_ENA	Management of TSF data – Writing of Initialization Data and Prepersonalization Data	No
FMT_MTD.1/INI_DIS	Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data	No
FMT_MTD.1/KEY_WRITE	Management of TSF data – Key Write	No
FMT_MTD.1/KEY_READ	Management of TSF data – Key Read	No
FPT_EMSEC.1	TOE Emanation	Yes
FPT_FLS.1	Failure with preservation of secure state	No
FPT_TST.1	TSF testing	Yes
FPT_PHP.3	Resistance to physical attack	No

6.1.2 Modified SFRs from the Protection Profile

The modifed SFRs are listed again in Table 19

Table 19. Modified Security Functional Requirements from the Protection Profile

SFR	Title
FCS_CKM.4	Cryptographic key destruction - MRTD
FCS_COP.1/SHA	Cryptographic operation – Hash for Key Derivation
FCS_COP.1/AUTH	Cryptographic operation – Authentication
FCS_RND.1	Quality metric for random numbers
FIA_UAU.4	Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE
FIA_UAU.5	Multiple authentication mechanisms
FIA_AFL.1	Authentication failure handling
FPT_EMSEC.1	TOE Emanation
FPT_TST.1	TSF testing

6.1.2.1 FCS_CKM.4

This Security Target performs two assignment operations on FCS_CKM.4 according to Application Note 19 in the Protection Profile [7].

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

FAU_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method*overwriting with a random byte*[1] that meets the following *none*[2] .

6.1.2.2 FCS_COP.1/SHA

This Security Target performs two selection operations on FCS_COP.1/SHA according to Application Note 20 in the Protection Profile [7].

FCS_COP.1/SHA	**Cryptographic operation – Hash for Key Derivation**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SHA	The TSF shall perform hashing in accordance with a specified cryptographic algorithm *SHA-1, SHA-224, SHA-256* [3] that meets the following *FIPS 180-4* [4] .

6.1.2.3 FCS_COP.1/AUTH

This Security Target performs two selection operations on FCS_COP.1/AUTH according to Application Note 22 in the Protection Profile [7].

FCS_COP.1/AUTH	**Cryptographic operation – Authentication**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AUTH	The TSF shall perform symmetric authentication – encryption and decryption in accordance with a specified cryptographic algorithm *Triple-DES* [5] and cryptographic key sizes *112, 128, 168, 192 or 256* bit [6] that meet the following: *NIST SP800-67* [7] .

6.1.2.4 FCS_RND.1

This Security Target performs two selection operations on FCS_RND.1

FCS_RND.1	**Generation of Random Numbers**
Hierarchical to:	No other components.
Dependencies:	No other dependencies

1 [assignment: *cryptographic key destruction method*]
2 [assignment: *list of standards*]
3 [selection: *SHA-1 or other approved algorithms]*]
4 [selection:*FIPS 180-2 or other approved standards*]
5 [selection: *Triple-DES, AES*]
6 [selection:*112, 128, 168, 192, 256*]
7 [selection:*FIPS 46-3, FIPS 197*]

FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet *AIS31 DRG.4 according to* [1] [8] .

6.1.2.5 FIA_UAU.4

This Security Target performs two selection operations on FIA_UAU.4 and adds a consideration for the Active Authentication Protocol

FIA_UAU.4	**Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE**
Hierarchical to:	No other components.
Dependencies:	No other Dependencies
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 *Triple-DES* [9] 3. Active Authentication Protocol

6.1.2.6 FIA_UAU.5

This Security Target performs two selection operations on FIA_UAU.5.

FIA_UAU.5	**Multiple authentication mechanisms**
Hierarchical to:	No other components.
Dependencies:	No other Dependencies
FIA_UAU.5.1	The TSF shall provide 1. Basic Access Control Authentication Mechanism 2. Symmetric Authentication Mechanism based on *Tripl e-DES* [10] 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 one of the following mechanism(s) *the Basic Access Control Authentication Mechanism with the Personalization Agent Keys* [11], 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.

8 [assignment: *a defined quality metric]*]
9 [selection: *Triple-DES, AES or other approved algorithms]*]
10 [selection: *Triple-DES, AES]*]
11 [selection:*the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key,* [assignment:*other*]]

6.1.2.7 FIA_AFL.1

This Security Target performs one selection and four assignment operations on FIA_AFL.1 according to Application Note 35 in the Protection Profile [7].

FIA_AFL.1	**Authentication Failure Handling**
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when *an administrator configurable positive integer within [1:256]* [12] unsuccessful authentication attempts occur related to *BAC Authentication* [13] .
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been *met* [14], the TSF shall *increase a processing delay time quadratically for each subsequent failing attempt, resetting the delay after a good attempt* [15].

6.1.2.8 FPT_EMSEC

This Security Target performs four assignment operations on FPT_EMSEC.1. The SFR has also adds protection against leakage on the Active Authentication private key

FPT_EMSEC.1	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No other Dependencies
FPT_EMSEC.1.1	The TOE Shall not emit *information of IC Power consumption* [16] in excess of *state of the art values* [17] enabling access to Personalization Agent Key(s) and *Active Authentication Private Key* [18].
FPT_EMSEC.1.2	The TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Key(s) and *Active Authentication Private Key* [19].

6.1.2.9 FPT_TST.1

This Security Target performs a selection and an assignment operation on FPT_TST.1 according to Application Note 46 in the Protection Profile [7].

FPT_TST.1	**TSF Testing**
Hierarchical to:	No other components.
Dependencies:	No Dependencies

12 [selection: [*assignment: positive integer number*], *an administrator configurable positive integer within [assignment: range of acceptable values]*]
13 [assignment:*list of authentication events*]
14 [assignment: *met or surpassed*]
15 [assignment: *list of actions*]
16 [assignment: *types of emissions*]
17 [assignment:*specified limits*]
18 [assignment: *list of types of user data*
19 [assignment: *list of types of user data*]

FPT_TST.1	The TSF shall run a suite of self tests *during initial startup (testing RNG) and during normal operation to detect Flash memory errors and during Crypto Library operations to mitigate Fault Analysis Attacks* [20] to demonstrate the correct operation of the TSF.

6.1.3 Additional SFRs

The SFRs described in this section are added to the Security Target in order to support the optional feature of Active Authentication

Table 20. Security Functional Requirements defined for optional Active Authentication

SFR	Title
FCS_COP.1/SHA	Cryptographic operation – Hash for Key Derivation
FCS_COP.1/SIG_GEN	Data Signature Generation using the AA Private Key
FCS_RND.1	Generation of Random Numbers
FIA_API.1	Active Authentication Protocol
FMT_MTD.1/AA	Active Authentication Keys access control

6.1.3.1 FCS_COP.1/SIG_GEN

This Security Target adds the refined SFR FCS_COP.1/SIG_GEN in order to support the Active Authentication mechanism

FCS_COP.1/SIG_GEN	**Cryptographic operation – Signature Generation**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SIG_GEN	The TSF shall perform *Digital Signature Generation* [21] in accordance with a specified cryptographic algorithm [22] *RSA or ECDSA* and cryptographic key sizes [23] *RSA 1024 to 4096 bits (in increments of 64 bits)*, *ECC 224 to 521* that meets the following [24] *ISO 9796-2*[12], *ANSI X9.62*[13].
Application Note	For signature generation in the Active Authentication mechanism, the TOE uses ISO/IEC 9796-2 compliant cryptography (scheme 1).

6.1.3.2 FIA_API.1

This Security Target adds FIA_API.1 in order to support the Active Authentication mechanism

20 [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]]
21 [assignment:*list of cryptographic operations*]
22 [assignment: *cryptographic algorithm*]
23 [assignment:*cryptographic key sizes*]
24 [assignment:*list of standards*]

FIA_API.1	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No other Dependencies
FIA_API.1	The TSF shall provide a *Active Authentication Protocol according to* [8] [25] to prove the identity of the *TOE* [26].

6.1.3.3 FMT_MTD.1/AA

This Security Target performs two selection operations on FMT_MTD.1 and adds a consideration for the Active Authentication Protocol

FMT_MTD.1/AA	**Management of TSF Data**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/AA	The TSF shall restrict the ability to *create* [27] the *Active Authentication Private Key* [28] to *the Personalization Agent*. [29]

6.2 SFR dependency Analysis

The Security Target SFR dependencies concur with the analyis provided in Section 6.3.2 of the Protection Profile, BSI-CC-PP0056 [7]

The dependency analysis for additional SFRs is provided in the table below

Table 21. SFR Dependency Analysis

SFR	Dependencies	Support
FCS_COP.1/SIG_GEN	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Unsupported
	FCS_CKM.4	Unsupported
FCS_COP.1/SHA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Unsupported
	FCS_CKM.4	Unsupported
FCS_RND.1	No Dependency	
FIA_API.1	No Dependency	
FMT_MTD.1/AA	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1

The rationale for unsupported dependencies is given below

25 [assignment: *authentication mechanism*]
26 [assignment: *authorized user or role*]
27 [selection: *change_default, query, modify, delete, clear]*[assignment: *other operations*]
28 [assignment:*list of TSF Data*
29 [assignment:*the authorised identified roles*

Table 22. Unsupported Dependencies

SFR	Rationale
FCS_COP.1/SIG_GEN	The SFR FCS_COP.1/SIG_GEN uses a key stored by the perso agent using FMT_MTD.1/KEY_WRITE, thus there is no need to generate or import a key during the addressed TOE lifecycle. Since the Key is stored permanently, there is no need for FCS_CKM.4 either.
FCS_COP.1/SHA	The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

6.3 Security Assurance Requirements for the TOE

The security assurance requirements defined by Section 6.2 of the Protection Profile, BSI-PP-CC-0055 [7] apply entirely to this Security Target.

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

- ALC_DVS: augmented from 1 to 2

6.4 Security Requirements Rationale

This rationale is available in the full version of the Security Target, available in certain cases only under NDA.

Table 23. Mapping of the Security Objectives for the TOE to the Security Functional Requirements for the TOE

Security Objective for the TOE	Security Functional Requirement of the TOE
OT.AC_Pers	FCS_CKM.1, FCS_CKM.4
	FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC, FCS_RND.1
	FIA_UAU.4, FIA_UAU.5, FIA_UAU.6
	FDP_ACC.1, FDP_ACF.1, FDP_UCT.1, FDP_UIT.1,
	FMT_SMF.1, FMT_SMR.1
	FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ
	FPT_EMSEC.1, FPT_FLS.1, FPT_PHP.3
OT.Data_Int	FCS_CKM.1, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC, FCS_RND.1
	FIA_UAU.4, FIA_UAU.5, FIA_UAU.6
	FDP_ACC.1, FDP_ACF.1, FDP_UCT.1, FDP_UIT.1
	FMT_SMF.1, FMT_SMR.1,
	FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ
OT.Data_Conf	FCS_CKM.1, FCS_CKM.4
	FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC, FCS_RND.1
	FIA_UID.1, FIA_AFL.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6

Security Objective for the TOE	Security Functional Requirement of the TOE
	FDP_ACC.1, FDP_ACF.1, FDP_UCT.1, FDP_UIT.1,
	FMT_SMF.1, FMT_SMR.1
	FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ
OT.Identification	FAU_SAS.1, FIA_UID.1, FIA_AFL.1, FIA_UAU.1
	FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS
OT.Prot_Inf_Leak	FPT_EMSEC.1, FPT_TST.1 FPT_FLS.1, FPT_PHP.3
OT.Prot_Phys_Tamper	FPT_PHP.3
OT.Prot_Malfunction	FPT_TST.1, FPT_FLS.1
OT.Prot_Abuse-Func	FMT_LIM.1, FMT_LIM.2
OT.AA_Proof	FCS_RND.1
	FCS_COP.1/SHA
	FCS_COP.1/SIG_GEN
	FIA_API.1
	FMT_MTD.1/AA

The green cells in Table 23 indicate how the PP maps it's security objectives for the TOE to the Security Functional Requirements for the TOE.

The blue cells map the additional Objective OT.AA_Proof to the SFRs which support this objective. The justification is given as follows:

OT.AA_Proof (Proof of MRTD's chip authenticity by Active Authentication) is ensured by the Active Authentication Protocol provided by FIA_API.1/AA enforcing the identification and authentication of the MRTD chip. The Active Authentication protocol requires 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 imported during Personalization.

7 TOE Summary Specification

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

7.1 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.

The function includes 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 initial Active Authentication Private Key (FMT_MTD.1/AA)
  - 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))
- 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)

This security functionality covers:

- FDP_ACC.1
- FDP_ACF.1
- FDP_UCT.1
- FDP_UIT.1
- FMT_MTD.1/AAPK
- FMT_MTD.1/INI_ENA
- FMT_MTD.1/INI_DIS
- FMT_MTD.1/KEY_WRITE
- FMT_MTD.1/KEY_READ
- FMT_SMR.1

7.2 SF.Manufacturer Authentication

The Manufacturer authenticates during the Manufacturing Phase of the TOE (FAU_SAS.1)

This user is able to authenticate with the Operating System to perform TOE Operating System (OS) personalization (MRTD IC pre-personalization). He is also able to read the Initialization Data (FIA_UAU.1, FIA_UID.1).

When the TOE is ready to be personalized, the Manufacturer will create the authentication data for the Personalization Agent and terminate this manufacturing stage.

7.3 SF.Card Personalization

This TSF provides MRTD's chip personalization functions to allow the Personalization Agent to .

- create and set the initial MRTD's LDS data (FMT_SMF.1)
- Write and Read EF.COM, EF.SOD, EF.DG1 to EF.DG16 (FDP_ACF.1.2 (1))
- Create initial Active Authentication Private Key (FMT_MTD.1/AA)
- Write Document Basic Access Keys (FMT_MTD.1/KEY_WRITE)
- Disable read access to initialization data for users (FMT_MTD.1/INI_DIS)

This security functionality covers:

- FMT_SMF.1
- FDP_ACF.1.2 (1)
- FMT_MTD.1/AA
- FMT_MTD.1/KEY_WRITE
- FMT_MTD.1/INI_DI

7.4 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 symmetric encryption using TDES in CBC mode with a key length of 112 bits (FCS_COP.1/ENC).

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).

This security functionality covers:

- FCS_COP.1/ENC
- FIA_UAU.1
- FIA_UAU.5
- FIA_UID.1
- FMT_SMR.1
- FPT_EMSEC.1

7.5 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_RND.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 [15] from the common master secret K_{Master} = K_{PICC} XOR K_{PCD} and a Send Sequence Counter SSC derived from r_{PICC} and r_{PCD} (FCS_CKM.1). 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 number of successive authentication failures, a command processing delay is introduced, which increments quadratically (ms) after each failed authentication effort(FIA_AFL.1).

This security functionality covers:

- FCS_CKM.1
- FCS_COP.1/SHA
- FCS_COP.1/AUTH
- FCS_COP.1/MAC
- FCS_RND.1
- FIA_AFL.1
- FIA_UAU.1
- FIA_UAU.4
- FIA_UAU.5
- FIA_UID.1
- FMT_SMR.1

7.6 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 2.1 of [16].

This TSF involves an optional asymmetric Key Pair (KPrAA, KPuAA) which public part is stored in DG15 and private part is stored securely within the chip. This Key pair is imported to the MRTD during Personalisation.

This TSF ensures that the chip has not been substituted, by means of a challengeresponse protocol between the inspection system and the MRTD's chip. The TOE generates challenge data with a true random generated by the TOE (FCS_RND.1). The use of challenges enforces a protection against replay (FIA_UAU.4/AA). The TOE combines and hashes the challenge data(FCS_COP.1/SHA) with a terminal challenge before returning the signature (FCS_COP.1/SIG_GEN) to the Terminal. Where the

Signature scheme is RSA the hash size is indicated in the padding and for ECDSA, the hash size is stored in DG14.

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).

This security functionality covers:

- FCS_RND.1
- FCS_COP.1/SIG_GEN
- FCS_COP.1/SHA
- FIA_API.1
- FIA_UAU.4
- FMT_SMR.1
- FPT_EMSEC.1

7.7 SF.Secure Messaging

Commands and responses are exchanged between the TOE and the external device. This TSF provides a secure mean for the terminal and the card to exchange data (FIA_UAU.1, FIA_UAU.5): such as (and not restricted to) EF.COM, EF.SOD, EF.DG1 to EF.DG16.

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

This function enforces confidentiality (FDP_UCT.1) and integrity (FDP_UIT.1) of the transferred data (transmitted and received):

- Confidentiality is ensured by a TDES encryption (FCS_COP.1/ENC)
- Integrity is achieved by calculation, embodiment and verification of a Retail 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 destroyed the session keys (FCS_CKM.4). A session is also terminated upon reset of the TOE. A re-authentication using the BAC Authentication protocol is required after termination of a Secure Messaging session (FIA_UAU.6).

This security functionality covers:

- FCS_CKM.4
- FCS_COP.1/SHA
- FCS_COP.1/MAC
- FDP_UCT.1
- FDP_UIT.1
- FIA_UAU.1
- FIA_UAU.5
- FIA_UAU.6

7.8 SF.Crypto

This Security Function is responsible for providing cryptographic support to all the other Security Functions including secure key generation, secure random generator, and data hashing:

- Data hashing using SHA-1, SHA-224, SHA-256 (FCS_COP.1/SHA)
- RSA Sign and Verify operations with both CRT and standard Key Pairs of length 1024, 1280, 1536, 2048 bits (FCS_COP.1/SIG_GEN)
- TDES 2 Keys and 3 Keys in CBC and ECB modes (FCS_COP.1/ENC, FCS_COP.1/MAC, FCS_COP.1/AUTH)
- Secure destruction of cryptographic key secret or private material (FCS_CKM.4).
- The random number generator of the underlying IC is used by the TOE whenever the generation of a nonce is required (FCS_RND.1).
- Adequate number of Rabin Miller test rounds is performed in addition to GCD test in order to ensure correct generation of primes.
- MAC is generated and verified using TDES with 2 or 3 keys
- BAC protocol related cryptography (FCS_CKM.1/BAC)

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)

This security functionality covers:

- FCS_CKM.1
- FCS_CKM.4
- FCS_COP.1/SHA
- FCS_COP.1/ENC
- FCS_COP.1/MAC
- FCS_COP.1/AUTH
- FCS_COP.1/SIG_GEN
- FCS_RND.1
- FPT_EMSEC.1

7.9 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 (Biometrics, secret and private keys) when relevant memory is de-allocated (FCS_CKM.4)
- Validating the integrity of all stored cryptographic keys before use and informing the Terminal when such validation fails (FPT_TST.1).
- Ensuring that Information is not leaked.
- 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)

This security functionality covers:

- FCS_CKM.4
- FLT_LIM.1

- FLT_LIM.2
- FMT_SMF.1

8 Bibliography

8.1 Evaluation documents

[1] A proposal for: Functionality classes for random number generators, Wolfgang Killmann, T-Systems GEI GmbH, Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.0, 18 September 2011.

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001, April 2017.

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017.

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017.

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

[6] Security IC Platform Protection Profile with Augmentation Packages, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014.

[7] Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control (BAC PP), certified under the reference BSI-CC-PP-0055-2009, Version 1.10, BSI-CC-PP-0055.

[8] ICAO Doc9303, Machine Readable Travel Documents, 7th Edition, 2015.

8.2 Developer documents

[9] SmartePP User manual and administrator guide; Revision 1.4, 11 November 2020 .

[10] SmartePP ICAO Personalization Guide; Revision 1.4, 09 December 2020 .

[11] Security Target Lite, NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2), Rev. 1.8, 19 January 2021, NXP Semiconductors..

8.3 Standards

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

[13] 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.

9 Legal information

9.1 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.

9.2 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 and its suppliers accept 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.

9.3 Trademarks

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

Tables

Figures

Contents

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

Date of release: 2 March 2021
Document identifier: NXP-ST02-Smart_ePP-BAC