NXP SmartePP on P71 - ICAO EAC with SAC/PACE

Security Target - Lite

Rev. 1.4 — 2 March 2021 Product evaluation document

NSCIB-20-0108263

Document information

Information	Content
Keywords	Security Target, ICAO, Enhanced Access Control (EAC)
Abstract	Security Target for NXP Smart ePP Product on NXP P71 Certified Hardware, implementing an ICAO ePP with Extended Access Control (EAC)

Revision History

Revision history

Revision number	Date	Description
1.0	11 December 2020	Release version
1.1	18 December 2020	Update Cover sheet to reflect public version
1.2	08 January 2021	Update Table 1
1.3	26 Feb 2021	Correction in Table 4 and Bibliography

1 Introduction

1.1 ST Reference

Table 1. ST References

Title	Security Target Lite NXP SmartePP on P71 - ICAO EAC with SAC/ PACE
Version	1.4
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 Profiles	Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), certified under the reference BSI-CC-PP-0056-V2-2012-MA-02, Version 1.3.2 [7] Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), certified under the reference BSI-CC-PP-0068-V2-2011-MA-01, Version 1.01 [8]
Assurance Level	EAL5 augmented by AVA_VAN.5, ALC_FLR.1, ALC_DVS.2

1.1.1 TOE Reference

The TOE identity may be confirmed by retrieving the tags listed in using a GET DATA command as described in the SmartePP UGM [13], section 2.1

Table 2. 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

1.2 TOE Overview

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) DOC 9303 [10]. The Terms MRTD and Travel Document are used interchangeably in this document, using text derived from the Protection Profiles.

This ST extends this PP to contact, contactless and dual interface smartcard modules. It addresses the advanced security methods:

- Extended Access Control (EAC), including Chip Authentication
- Supplemental Access Control (SAC) also known as "Password Authenticated Connection Establishment" (PACE)

- as defined in BSI TR-03110 [12].

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) of ICAO DOC 9303 [10]. 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 [10]. 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 Extended Access Control (EAC) Mechanism.

This security target addresses the Chip Authentication Version 1 described in TR-03110 as an alternative to the Active Authentication stated in ICAO DOC 9303 [10].

This TOE addresses the ICAO defined security mechanisms

- Active Authentication
- Chip Authentication
- PACE

as optional.

1.2.2 Proprietary Features

1. Hardware Authentication: If enabled during the personalisation process a Mutual Authentication mechanism, that makes use of a dedicated Hardware platform feature, is supported.
2. Restricted Mode: If the Platform Attack Counter expires, Smart_ePP will enter a Restricted Mode which limits the TOE functionality. This may be exited by a successful Hardware Authentication.

1.3 TOE Definition - Physical Scope of the TOE

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, smart_ePP, programmed with the Logical Data Structure (LDS) providing Extended Access Control (EAC) and optional features Supplemental Access Control (SAC) and Chip Authentication defined by BSI Technical Guideline TR-03110 [12].

The TOE comprises:

- the circuitry of the MRTD's chip ([15]
- the IC Dedicated Software and Crypto Library ([15]
- the IC Embedded Software (SmartePP)
- a personalised filesystem, created in accordance with the guidance given
- the associated guidance documentation

Most ePassport products are primarily provisioned with Basic Access Control (BAC), to create the initial terminal session. BAC does not meet the cryptographic requirements to be considered resistant to attackers with a high attack potential, therefore some schemes may optionally use Supplemental Access Control (SAC) also known as 'Password Authenticated Connection Establishment' (PACE), which can achieve a higher attack rating.

Extended Access Control (EAC) requires that an initial terminal session is established before the EAC session may be established and is used to control access to more sensitive data groups.

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 security feature that may be 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, ICAO Doc 9303 [10], normative appendix 5.

No security claims for BAC are made in this Security Target

1.3.3 Password Authenticated Connection Establishment

This TOE optionally offers an optional security mechanism called PACE, which is designed to replace Basic Access Control (BAC) and is mandatory in many new e-passports.

For the PACE protocol according to ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.1, April 2014 [11], the following steps shall be performed:

1. the travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN [1] data and transmits the encrypted nonce together with the domain parameters to the terminal.
2. The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.
3. The travel document's chip and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the shared secret.
4. Each party generates an authentication token, sends it to the other party and verifies the received token. After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging).

1.3.4 Extended Access Control

The Extended Access Control consists of two parts

1. the Chip Authentication Protocol Version 1 and
2. the Terminal Authentication Protocol Version 1 (v.1)

The Chip Authentication Protocol version 1

1. authenticates the travel document’s chip to the inspection system and
2. establishes secure messaging which is used by Terminal Authentication v.1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system.
   Therefore Terminal Authentication v.1 can only be performed if Chip Authentication v.1 has been successfully executed.

The Terminal Authentication Protocol version 1 produces the following results:

1. the authentication of the inspection system as entity authorized by the receiving State or Organisation through the issuing State, and
2. an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems.
   The issuing State or Organisation authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

1.4 TOE Components and Composite Certification

The TOE is a composite product with the underlying Security IC being an NXP Flash based Secure Microcontroller N7121 [15] certified along with the embedded Security firmware and Cryptographic Libraries in accordance with BSI to EAL 6+.

Table 3. 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)

[1] Card Access Number

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.

1.5 TOE Lifecycle

The TOE Lifecycle is fully described in the composite product Protection Profile, BSI-CC-PP0055 [9], with reference to the PP0035, 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 [15].

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 cannot be modified, unless in the cases allowed by ICAO (LDS 2.0 MRTDs, specified from ICAO document 9303 revision 8). The Operational Use phase is not part of the scope of this TOE.

1.6 TOE Delivery

The TOE delivery comprises the following items:

Table 4. TOE Delivery Items

Type	Name	Version	Form
Product	SmartePP on P71	03 00 00 10	NXP Secure Smart Card Controller N7121 including on-chip security software and Crypto Library and the SmartePP application
Document	SmartePP User manual and administrator guide	[13]	DocStore Document
Document	SmartePP ICAO Personalization Guide	[14]	DocStore Document

1.7 TOE Identification

The TOE identify may be confirmed by retrieving the tags listed in using a GET DATA command as described in the SmartePP UGM [13], section 2.1

Table 5. TOE References

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

1.8 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 ConformanceClaims

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 defined in the Protection Profiles are reused:

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

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”, Extended Access Control with PACE (EAC PP), certified under the reference BSI-CC-PP-0056-V2-2012-MA-02, Version 1.3.2[7]. This EAC PP [7] is also wholly compliant with the Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), certified under the reference BSI-CC-PP-0068-V2-2011-MA-01, Version 1.01 [8]

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 Section 4.1.

2.3 Package Claim

The assurance level for the TOE is CC EAL 5 augmented with

- AVA_VAN.5 'Advanced Methodical Vulnerability Analysis'
- ALC_DVS.2 'sufficiency of security measures'
- ALC_FLR.1 'Basic Flaw Remediation'

3 Security Problem Definition

3.1 SPD Introduction

The Security Problem definition of the Protection Profile, BSI-CC-PP-0056-V2-2012 [7] apply entirely to this Security Target.

3.1.1 Assets

The Assets described in section 3.1 of the Protection Profile, BSI-CC-PP-0056-V2-2012 [7] entirely apply to this Security Target and are listed in Table 6 .

Table 6. Assets defined in the Protection Profile

Name
Logical travel document sensitive User Data
Authenticity of the travel document’s chip

3.1.2 Subjects

The Subjects described in section 3.1 of the Protection Profile, PP0056 [7] entirely apply to this Security Target and are listed in Table 7.

Table 7. Subjects defined in the EAC Protection Profile

EAC Subjects
Country Verifying Certification Authority
Document Verifier
Terminal
Inspection system (IS)
MRTD Holder
Traveler
Attacker

All of the subjects defined in the PACE Protection Profile [8] also apply entirely to this Security Target.

Table 8. Subjects defined in the PACE Protection Profile

PACE Subjects
travel document holder
travel document presenter(traveller)
Basic Inspection System with PACE (BIS-PACE)
Document Signer (DS)
Country Signing Certification Authority (CSCA)
Personalisation Agent
Manufacturer
Traveler

PACE Subjects
Attacker

One additional Subject is defined, as the Hardware Authentication Administrator (S.HWAuth) with access to Hardware specific ciphertexts generated during Personalisation. The protocol overseen by S.HWAuth is described in Section 9 of [14]

S.HWAuth	**Administrator with access to Hardware Authentication Ciphertexts**

3.2 Assumptions

The Assumptions described in section 3.2 of the Protection Profile [7]entirely apply to this Security Target.

Table 9. Assumptions reused from the Protection Profile

Name	Title
A.Insp_Sys	Inspection Systems for global interoperability
A.Auth_PKI	PKI for Inspection Systems

The Assumptions described in section 3.2 of the PACE Protection Profile [8] also entirely apply to this Security Target.

Table 10. Assumptions defined in the PACE Protection Profile

Name	Title
A.Passive_Auth	PKI for Passive Authentication

3.3 Threats

The Threats described in section 3.2 of the Protection Profile, PP0056 [7]entirely apply to this Security Target. They are listed in Table 11.

Table 11. Threats against the TOE defined in the EAC Protection Profile

Name	Title
T.Read_Sensitive Data	Read the sensitive biometric reference data
T.Counterfeit	Counterfeit travel document chip data

Section 3.2 of the Protection Profile, PP0056 [7] also references those threats listed in Section 3.3 of the PP0068 [8], these also entirely apply to this Security Target. They are listed in Table 12.

Table 12. Threats against the TOE defined in the PACE Protection Profile

Name	Title
T.Skimming	Skimming travel document / Capturing Card-Terminal Communication
T.Eavesdropping	Eavesdropping on the communication between the TOE and the PACE Terminal
T.Tracing	Tracing Travel Document
T.Abuse-Func	Abuse of Functionality

Name	Title
T.Information_Leakage	Information Leakage from MRTD's chip
T.Phys-Tamper	Physical Tampering
T.Forgery	Forgery of Data
T.Malfunction	Malfunction due to Environmental Stress

3.3.1 Restricted Mode

T.Restricted_Mode

Threat to Restricted Mode

Unauthorized user uses Hardware Authentication to exit Restricted Mode - threatens all assets as Restricted Mode is a response to undefined behaviour.

3.4 Organisational Security Policies

The Organisation Security Policies described in section 3.4 of the Protection Profile, BSI-CC-PP-0056-V2-2012 [7] entirely apply to this Security Target.

Table 13. Standard OSPs defined in the Protection Profile

Name	Title
P.Sensitive_Data	Privacy of sensitive biometric reference data
P.Personalization	Personalization of the MRTD by issuing State or Organization only

Section 3.4 of the Protection Profile PP0056 [7] also references those OSP's listed in Section 3.3 of the PP0068 [8], these also entirely apply to this Security Target. They are listed in Table 14

Table 14. Standard OSPs defined in the Protection Profile

Name	Title
P.Manufact	Manufacturing of the travel document’s chip
P.Pre-Operational	Pre-operational handling of the travel document
P.Card_PKI	PKI for Passive Authentication (issuing branch)
P.Trustworthy_PKI	Trustworthiness of PKI
P.Terminal	Abilities and trustworiness of Terminals

4 Security Objectives for the TOE

4.1 Security Objectives for the TOE

The Security Objectives for the TOE detailed in Section 4.1 of the Protection Profile [7] apply entirely to this Security Target, listed in Table 15 .

A further security Objective for the TOE, OT.AA_Proof, is included to address the optional Active Authentication feature.

Table 15. Security Objectives for the TOE defined in the EAC Protection Profile

Name	Title
OT.Sens_Data_Conf	Confidentiality of sensitive biometric reference data
OT.Chip_Auth_Proof	Proof of the travel document's chip authenticity

The PP also references those Security Objectives for the TOE listed in Section 4.1 of the (PACE PP), these also entirely apply to this Security Target. They are listed in Table 16

Table 16. Security Objectives for the TOE defined in PACE PP

Name	Title
OT.Data_Integrity	Integrity of Personal Data
OT.Data_Authenticity	Authenticity of Data
OT.Data_Confidentiality	Confidentiality of personal data
OT.Tracing	Tracing travel document
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
OT.Identification	Identification of the TOE
OT.AC_Pers	Access Control for Personalisation of logical MRTD

4.2 Security Objectives for the Operational Environment

The Security Objectives for the Operational Environment detailed in Section 4.2 of the Protection Profile, PP0056 [7] apply entirely to this Security Target and are listed in Table 17.

Table 17. Security objectives for the Operational Environment defined in the EAC Protection Profile

Name	Title
OE.Auth_Key_Travel_Document	Travel Document Authentication Key
OE.Authoriz_Sens_data	Authorization for Use of Sensitive Biometric Reference Data
OE.Exam_Travel_Document	Examination of the physical part of the travel document
OE.Prot_Logical_Travel_Document	Protection of data from the logical travel document

Name	Title
OE.Ext_Insp_Systems	Authorization of Extended Inspection Systems

The PP also references those Security Objectives for the Operational Environment listed in Section 4.2 of the PP0068, [8], these also entirely apply to this Security Target. They are listed in Table 18.

Table 18. Security objectives for the Operational Environment defined in the PACE Protection Profile

Name	Title
OE.Legislative_Compliance	Issuing of the Travel Document
OE.Passive_Auth_Sign	Authentication of travel document by signature
OE.Personalisation	Personalisation of travel document
OE.Terminal	Terminal operating
OE.Travel_Document_ Holder	Travel Document holder Obligation

4.3 Security Objectives Rationale

The rationale for the Security Objectives provided in Section 4.3 of the Protection Profile, PP0056 [7] apply entirely to this Security Target.

The Security objective OT.AA_Proof is included as an additional means of mitigating the Threat T.Counterfeit.

The Additional Security objective OT.Restricted_Mode is included as an means of mitigating the Threat T.Restricted_Mode.

4.3.1 Rationale for Active Authentication

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

4.3.2 Rationale for Restricted Mode

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

5 Extended Components

Extended Components defined in the EAC Protection Profile, PP0056 [7] apply entirely to this Security Target. The EAC PP also reuses Extended Components defined in the PACE Protection Profile, [8], which also apply entirely to this Security Target.

Table 19. Extended Components defined in the PACE Protection Profile

Name	Title
FAU_SAS	Audit Data Storage
FCS_RND	Generation of random numbers
FMT_LIM	Limited capabilities and availability
FPT_EMS	TOE Emanation

Table 20. Extended Components defined in the EAC Protection Profile

Name	Title
FIA_API	Authentication Proof of Identity

6 Security Requirements

This Security Target maintains complete consistency with the description of the CC operations given in Section 6 of [7].

This Security Target uses the security attribute definitions described in Section 6 of the PP [7], adding the platform error counter as an attribute. The platform error counter is referred to as 'attack counter' throughout the SmartePP documentation and when it expires puts the TOE into Restricted Mode.

Table 21. Additional Security Attributes

Security Attribute	Values	Meaning
Attack-Counter	[1:100]	Counter value

6.1 Security Functional Requirements for the TOE

This security functional requirements defined by Section 6.1 of the Protection Profile [7] apply entirely to this Security Target. This security target follows the precedent set in that Protection Profile of listing the PACE SFRs first then documenting those SFRs which are modified by the permitted operations.

6.1.1 SFRs from the PACE Protection Profile

Table 22. Security Functional Requirements from the PACE Protection Profile

SFR	Title	Modified
FAU_SAS.1	Audit Storage	No
FCS_CKM.1/DH_PACE	Cryptographic key generation – Diffe-Hellman for PACE Session	Yes
FCS_CKM.4	Cryptographic key destruction - Session Keys	Yes
FCS_COP.1/PACE_ENC	Cryptographic operation – Hash for Key Derivation	Yes
FCS_COP.1/PACE_MAC	Cryptographic operation – Encryption / Decryption	Yes
FCS_RND.1	Quality metric for random numbers	Yes
FIA_AFL.1/PACE	Authentication failure handling – PACE authentication using non-blocking authorisation data	Yes
FIA_UAU.6/PACE	Re-authenticating of Terminal by the TOE	No
FDP_RIP.1	Subset residual information protection	Yes
FDP_UCT.1/TRM	Basic data exchange confidentiality – MRTD	No
FDP_UIT.1/TRM	Data Exchange integrity	No
FMT_SMF.1	Specification of Management Functions	No
FMT_MTD.1/INI_ENA	Management of TSF data – Writing Initialisation and Pre-personalisation Data	No
FMT_MTD.1/INI_DIS	Management of TSF data – Reading and Using Initialisation and Pre-personalisation Data	No
FMT_MTD.1/PA	Management of TSF data – Personalisation Agent	No

SFR	Title	Modified
FPT_TST.1	TSF testing	Yes
FPT_FLS.1	Failure with preservation of secure state	Yes
FPT_PHP.3	Resistance to physical attack	No
FTP_ITC.1/PACE	Inter-TSF trusted channel after PACE	No

6.1.2 SFRs from the PACE Protection Profile - modified

Table 23. Modified Security Functional Requirements from the PACE Protection Profile

SFR	Title
FCS_CKM.1/DH_ PACE	Cryptographic key generation – Diffe-Hellman for PACE Session
FCS_CKM.4	Cryptographic key destruction - Session Keys
FCS_COP.1/PACE_ ENC	Cryptographic operation – Encryption / Decryption AES / 3DES
FCS_COP.1/PACE_ MAC	Cryptographic operation – Encryption / Decryption
FCS_RND.1	Quality metric for random numbers
FIA_AFL.1/PACE	Authentication failure handling – PACE authentication using non-blocking authorisation data
FDP_RIP.1	Subset residual information protection
FPT_TST.1	TSF testing
FPT_FLS.1	Failure with preservation of secure state

6.1.2.1 FCS_CKM.1/DH_PACE

This refinement of the SFR FCS_CKM.1

FCS_CKM.1/DH_PACE **Cryptographic key generation - Diffie-Hellman for PACE session keys**

Hierarchical to: No other components.

Dependencies: [*FCS_CKM.2 Cryptographic key distribution or* [2] FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction : fulfilled by FCS_CKM.4

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Diffie-Hellman Protocol compliant to PKCS#3 or ECDH compliant to TR-03111* [21] [3] and specified cryptographic key sizes *RSA 1024-1536-2048 or EC$_{brainpool}$192-224-256-320-384-512 or EC$_{NIST}$192-224-256-384-521* [4] that meet the following: *[ICAO_SAC]* [11] [5].

[2] A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case

[3] [assignment: *cryptographic key generation algorithm*]

[4] [assignment: *cryptographic key sizes*]

[5] [assignment: *list of standards*]

6.1.2.2 FCS_CKM.4

This Security Target performs two assignment operations on FCS_CKM.4 according to Application Note 28 in the Protection Profile PP0068 [8].

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]: fulfilled by FCS_CKM.1/DH_PACE
FAU_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting with a random byte* [6] that meets the following *none* [7] .

6.1.2.3 FCS_COP.1/PACE_ENC

This Security Target performs two selection operations on FCS_COP.1/PACE_ENC according to Application Note 29 in the Protection Profile [8].

FCS_COP.1/PACE_ENC	**Cryptographic operation – Encryption / Decryption AES / 3DES**
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/PACE_ENC	The TSF shall perform secure messaging - encryption and decryption in accordance with a specified cryptographic algorithm *AES, 3DES (TDES)* in CBC mode [8] and cryptographic key sizes *112, 128, 192, 256* [9] that meets the following *[ICAO-SAC]* [11]

6.1.2.4 FCS_COP.1/PACE_MAC

This Security Target performs two selection operations on FCS_COP.1/PACE_MAC according to Application Note 29 in the Protection Profile [8].

FCS_COP.1/PACE_MAC	**Cryptographic operation – MAC**
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/PACE_MAC	The TSF shall perform secure messaging - - message authentication code in accordance with a specified cryptographic algorithm *CMAC, Retail-MAC* [10] and

[6] [assignment: *cryptographic key destruction method*]

[7] [assignment: *list of standards*]

[8] [selection: AES, 3DES] in CBC mode

[9] [selection:*112, 128, 192, 256*]

[10] [selection: CMAC, Retail-MAC]

	cryptographic key sizes *112, 128, 192, 256* [11] that meets the following: compliant to [ICAO-SAC] [11]

6.1.2.5 FCS_RND.1

This Security Target performs one selection operations on FCS_RND.1 according to Application Note 31 in the Protection Profile [8].

FCS_RND.1	**Generation of Random Numbers**
Hierarchical to:	No other components.
Dependencies:	No other dependencies
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet *AIS31 DRG.4 according to* [1]*[KS2011]* [12] .

6.1.2.6 FIA_AFL.1/PACE

This Security Target performs two assignment operations on FIA_AFL.1/PACE according to Application Note 32 in the Protection Profile [8].

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 range 1-256* [13] unsuccessful authentication attempts occur related to authentication attempts using the PACE password as shared password .
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].

6.1.2.7 FDP_RIP.1

This Security Target performs two assignment operations on FDP_RIP.1 according to Application Note 42 in the Protection Profile [8].

FDP_RIP.1	**Subset residual information protection**
Hierarchical to:	No other components.
Dependencies:	No Dependencies
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* [16] from the following objects:

[11] [selection:*112, 128, 192, 256*]

[12] [assignment: *a defined quality metric*]

[13] [assignment: *positive integer number*]

[14] [assignment: *met or surpassed*]

[15] [assignment: *list of actions*]

[16] [selection:*allocation of the resource to, deallocation of the resource from*]

1. Session Keys (immediately after closing related communication session)
2. the ephemeral private key ephem-SK$_{PICC}$-PACE (by having generated a DH shared K (according to [ICAO_SAC] [11]
3. none

[17]

6.1.2.8 FPT_TST.1

This Security Target performs a selection and an assignment operation on FPT_TST.1 according to Application section 6.1.6.4 in the Protection Profile [8].

FPT_TST.1	**TSF Testing**
Hierarchical to:	No other components.
Dependencies:	No Dependencies
FPT_TST.1.1	The TSF shall run a suite of self tests *during initial startup (testing RNG) and during normal operation to detect Flash memory errors and during Crypto Library operations to mitigate Fault Analysis Attacks* [18] 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 the TSF Data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code

6.1.2.9 FPT_FLS.1

This Security Target uses the refinement of FPT_FLS.1 specified in [8].

FPT_FLS.1	**TSF Testing**
Hierarchical to:	No other components.
Dependencies:	No Dependencies
FPT_FLS.1	The TSF shall preserve a secure state when the following types of failures occur:

1. Exposure to Operating conditions causing a TOE malfunction
2. failure detected by TSF according to FPT_TST.1
3. none

[19]

[17] [assignment: *list of objects*

[18] [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*]]

[19] [assignment: *list of types of failures in the TSF*

6.1.3 SFRs from the EAC Protection Profile

Table 24. Security Functional Requirements from the EAC Protection Profile

SFR	Title	Modified
FCS_CKM.1/CA	Cryptographic key generation – Diffie-Hellman for Chip Authentication	Yes
FCS_COP.1/CA_ENC	Cryptographic operation – Symmetric Encryption / Decryption	Yes
FCS_COP.1/SIG_VER	Cryptographic operation – Signature Verification by travel document	Yes
FCS_COP.1/CA_MAC	Cryptographic operation – MAC	Yes
FIA_UID.1/PACE	Timing of identification	Yes
FIA_UAU.1/PACE	Timing of authentication	Yes
FIA_UAU.4/PACE	Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE	Yes
FIA_UAU.5/PACE	Multiple authentication mechanisms	Yes
FIA_UAU.6/EAC	Re-authenticating – Re-authenticating of Terminal by the TOE	No
FIA_API.1	Authentication Proof of Identity	No
FDP_ACC.1/TRM	Subset access control – Basic Access control	No
FDP_ACF.1/TRM	Basic Security attribute based access control – Basic Access Control	No
FMT_SMR.1/PACE	Security roles	No
FMT_LIM.1	Limited capabilities	No
FMT_LIM.2	Limited availability	No
FMT_MTD.1/CVCA_INI	Management of TSF data – Initialization of CVCA Certificate and Current Date	Yes
FMT_MTD.1/CVCA_UPD	Management of TSF data – Country Verifying Certification Authority	No
FMT_MTD.1/DATE	Management of TSF data – Current Date	No
FMT_MTD.1/CAPK	Management of TSF data – Chip Authentication Private Key	Yes
FMT_MTD.1/KEY_READ	Management of TSF data – Key Read	No
FMT_MTD.3	Secure TSF data	No
FPT_EMS.1	TOE Emanation	Yes

6.1.4 SFRs from the EAC Protection Profile - modified

The modifed SFRs are listed in Table 25

Table 25. Modified Security Functional Requirements from the EAC Protection Profile

SFR	Title
FCS_CKM.1/CA	Cryptographic key generation – Diffie-Hellman for Chip Authentication

SFR	Title
FCS_COP.1/CA_ENC	Cryptographic operation – Symmetric Encryption / Decryption
FCS_COP.1/SIG_VER	Cryptographic operation – Signature verification by travel document
FCS_COP.1/CA_MAC	Cryptographic operation – MAC
FIA_API.1	Authentication Proof of Identity
FIA_UAU.1/PACE	Timing of authentication
FIA_UAU.4/PACE	Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE
FIA_UAU.5/PACE	Multiple authentication mechanisms
FIA_UAU.6/EAC	Re-authenticating – Re-authenticating of Terminal by the TOE
FIA_UID.1/PACE	Timing of Identification
FMT_MTD.1/CVCA_INI	Management of TSF data – Initialization of CVCA Certificate and current date
FPT_EMS.1	TOE Emanation

6.1.4.1 FCS_CKM.1/CA

This refinement of the SFR FCS_CKM.1

FCS_CKM.1/CA	**Cryptographic key generation - Diffie-Hellman for Chip Authentication**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/CA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Diffie-Hellman Protocol compliant to PKCS#3* [20] *or ECDH compliant to [TR-03111]* [21] [20] and specified cryptographic key sizes *RSA 1024-1536-2048 or EC$_{brainpool}$192-224-256-320-384-512 or EC$_{NIST}$192-224-256-384-521* [21] that meet the following: [20], [21] *and* [22] . [22]

6.1.4.2 FCS_COP.1/CA_ENC

This Security Target performs two selection operations on FCS_COP.1/CA_ENC according to Application Note 16 in the Protection Profile [7].

FCS_COP.1/CA_ENC	**Cryptographic operation – Symmetric Encryption / Decryption**
Hierarchical to:	No other components.

[20] [assignment: *cryptographic key generation algorithm*]

[21] [assignment: *cryptographic key sizes*]

[22] [selection: *based on the Diffie-Hellman key derivation protocol compliant to [PKCS#3]* [20] *and [TR-03110_EAC]* [22] *based on an ECDH protocol compliant to [TR-03111]* [21]]

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/CA_ENC	The TSF shall perform secure messaging - encryption and decryption in accordance with a specified cryptographic algorithm *AES, 3DES (TDES) in CBC mode* [23] and cryptographic key sizes *112, 128, 192 or 256* [24] that meets the following: *[TR-03110_EAC]* [22]

6.1.4.3 FCS_COP.1/CA_MAC

This Security Target performs two selection operations on FCS_COP.1/CA_MAC according to Application Note 29 in the Protection Profile [8].

FCS_COP.1/CA_MAC	**Cryptographic operation – MAC**
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/CA_MAC	The TSF shall perform secure messaging - message authentication code in accordance with a specified cryptographic algorithm *Retail MAC (DES) and CMAC (AES)* [25] and cryptographic key sizes 112, 128, 192 or 256 [26] that meets the following: *complies with TR-03110-3* [19]

6.1.4.4 FCS_COP.1/SIG_VER

This Security Target performs two selection operations on FCS_COP.1/PACE_ENC according to Application Note 29 in the Protection Profile [8].

FCS_COP.1/SIG_VER	**Cryptographic operation – Signature verification by travel document**
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_VER	The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm *RSA or ECDSA* [27] and cryptographic key sizes RSA 1024-1280-1536-2048-4096 bits or ECDSA 192-224-256-384-521 bits respectively [28] that meets the following: *complies with [TR-03110-3]* [19]

[23] [assignment: *cryptographic algorithm*]

[24] [assignment:*112, 128, 192, 256*]

[25] [assignment: *cryptographic algorithm*

[26] [assignment:*112, 128, 192 or 256*]

[27] [assignment: cryptographic algorithm]

[28] [assignment:*cryptographic key sizes*]

6.1.4.5 FIA_UID.1/PACE

This Security Target performs two selection operations on FIA_UID.1/PACE

FIA_UID.1/PACE **Timing of Authentication**

Hierarchical to: No other components.

Dependencies: No other Dependencies

FIA_UID.1.1/PACE The TSF shall allow:

1. to establish the communication channel
2. carrying out the PACE Protocol according to [11]
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
4. to carry out the Chip Authentication Protocol Version 1 according to [18]
5. to carry out the Terminal Authentication Protocol Version 1 according to [18]
6. [29] *to carry out the Active Authentication mechanism according to* [10]

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/PACE The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.6 FIA_UAU.1/PACE

This Security Target performs an assignment operation on FIA_UAU.1/PACE

FIA_UAU.1/PACE **Timing of Authentication**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE

FIA_UAU.1.1 The TSF shall allow

1. to establish a communication channel
2. carrying out the PACE Protocol according to [11], [30]
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
4. to identify themselves by selection of the authentication key
5. to carry out the Chip Authentication Protocol Version 1 according to [18]
6. to carry out the Terminal Authentication Protocol Version 1 according to [18]
7. [31] *to carry out the Active Authentication mechanism according to* [10]

[29] [assignment: *list of TSF-mediated actions*]

[30] travel document identifies itself within the PACE protocol by selection of the authentication key ephem-PKPICC-PAC

[31] [assignment: *list of TSF-mediated actions*]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/PACE The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.7 FIA_UAU.4/PACE

FIA_UAU.4/PACE **Single-use authentication of the Terminal by the TOE**

Hierarchical to: No other components.

Dependencies: No other Dependencies

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

1. PACE Protocol according to [11]
2. Authentication Mechanism based on *AES* [32]
3. Terminal Authentication Protocol Version 1 according to [18]
4. Active Authentication[33]

6.1.4.8 FIA_UAU.5/PACE

This Security Target performs one selection operation and one assignment operation on FIA_UAU.5/PACE according to Application Note 28 in the Protection Profile [7].

FIA_UAU.5/PACE **Multiple authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No Dependencies

FIA_UAU.5.1 The TSF shall provide

1. PACE Protocol according to [11]
2. Passive Authentication according to ICO DOC 9303 [10]
3. Secure messaging in MAC-ENC mode according to [11]
4. Symmetric Authentication Mechanism based on *AES or TDES* [34],
5. Terminal Authentication Protocol v.1 according to [18]

to support user authentication.

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

1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.

[32] [selection: *Triple-DES, AES or other approved algorithms*]]

[33] [assignment: *identified authentication mechanism(s)*]]

[34] [selection: *Triple-DES, AES or other approved algorithms*]

2. The TOE accepts the authentication attempt as Personalisation Agent by *Symmetric Authentication Mechanism with Personalization Agent Key.* [35].
3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.
4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1.
5. none [36]

6.1.4.9 FMT_MTD.1/CVCA_INI

This Security Target performs one assignment operation on FMT_MTD.1/CVCA_INI according to Application Note 45 in the Protection Profile [7].

FMT_MTD.1/CVCA_INI	**Management of TSF data – Initialization of CVCA Certificate and Current Date**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles
FMT_MTD.1/CVCA_INI	The TSF shall restrict the ability to write the 1. initial Country Verifying Certification Authority Public Key 2. initial Country Verifying Certification Authority Certificate 3. initial Current Date 4. none to *the manufacturer* [37].

Application note: The Manufacturer is the Module Manufacturer.

6.1.4.10 FMT_MTD.1/CAPK

This Security Target performs one assignment operation on FMT_MTD.1/CAPK according to Application Note 45 in the Protection Profile [7].

FMT_MTD.1/CAPK	**Management of TSF Data - Chip Authentication Key**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

[35] [selection: *the Authentication Mechanism with Personalisation Agent Key(s)*]
[36] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
[37] [assignment:*the authorised identified roles*]

FMT_MTD.1/CAPK The TSF shall restrict the ability to *create or load* [38] the Chip Authentication Private Key to *the Personalization Agent* [39].

6.1.4.11 FPT_EMS.1

This Security Target performs six assignment operations on FPT_EMS.1 according to Application Note 47 in the Protection Profile [7].

FPT_EMS.1 **TOE Emanation**

Hierarchical to: No other components.

Dependencies: No other Dependencies

FPT_EMS.1.1 The TOE Shall not emit *information of IC Power consumption or EM radiation* [40] in excess of *state of the art values* [41] enabling access to :

1. Chip Authentication Session Keys
2. PACE session Keys (PACE-K_{MAC}, PACE-K_{ENC})
3. The ephemeral private key SK$_{PICC}$-PACE
4. Personalisation Agent Key(s)
5. Chip Authentication Private Key, and Active Authentication Private Key[42]

and

1. Confidential User data[43]

FPT_EMS.1.2 The TSF shall ensure any users [44] are unable to use the following interface smart card circuit contacts [45] to gain access to:

1. Chip Authentication Session Keys
2. PACE session Keys (PACE-K_{MAC}, PACE-K_{ENC})
3. The ephemeral private key SK$_{PICC}$-PACE
4. Personalisation Agent Key(s)
5. Chip Authentication Private Key, and Active Authentication Private Key[46]

and

1. Confidential User data[47]

[38] [selection: *create, load*]

[39] [assignment:*the authorised identified roles*]

[40] [assignment: *types of emissions*]

[41] [assignment:*specified limits*]

[42] [assignment:*list of types of TSF data*]

[43] [assignment:*list of types of user data*

[44] [assignment: *type of users*

[45] [assignment: *type of connection*]

[46] [assignment:*list of types of TSF data*]

[47] [assignment:*list of types of user data*

6.1.5 Active Authentication SFRs

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

Table 26. Additional Security Functional Requirements for Active Authentication

SFR	Title
FCS_COP.1/SIG_GEN	Data Signature Generation using the AA Private Key
FIA_API.1/AAP	Active Authentication Protocol
FMT_MTD.1/AA	Active Authentication Keys access control
FCS_COP.1/SHA	SHA Hash
FIA_UAU.4/AA	Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

6.1.5.1 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* [48] in accordance with a specified cryptographic algorithm [49] *RSA or ECDSA* and cryptographic key sizes [50] *RSA 1024 to 4096 bits (in increments of 64 bits), ECC 224 to 521 that meets the following*, that meets the following [51] *ISO 9796-2*[16] *ANSI X9.62*[17]
Application Note	For signature generation in the Active Authentication mechanism, the TOE uses ISO/IEC 9796-2 compliant cryptography (scheme 1).

6.1.5.2 FIA_API.1/AA

FIA_API.1/AA	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No other Dependencies
FIA_API.1/AA	The TSF shall provide a *Active Authentication Protocol according to ICAO DOC 9303* [10] [52] to prove the identity of the *TOE* [53].

[48] [assignment:*list of cryptographic operations*]
[49] [assignment: *cryptographic algorithm*]
[50] [assignment:*cryptographic key sizes*]
[51] [assignment:*list of standards*]
[52] [assignment: *authentication mechanism*]
[53] [assignment: *authorized user or role*]

6.1.5.3 FIA_UAU.4/AA

This Security Target refines the SFR FIA_UAU.4 in order to apply to Active Authentication.

FIA_UAU.4/AA	**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/AA	The TSF shall prevent reuse of authentication data related to 1. Active Authentication Protocol *AA_ Authentication_method* [54] .

6.1.5.4 FMT_MTD.1/AA

This Security Target makes a refinement on FMT_MTD.1 to address the optional installation of the Active Authentication Private Keys

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* [55] the *Active Authentication Private Key* [56] to *the Personalization Agent*. [57]

6.1.5.5 FCS_COP.1/SHA

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 or SHA-256* [58] and cryptographic keysize <u>none</u>[59] that meets the following *FIPS 180-4* [60] .

6.1.6 Hardware Authentication SFRs

The SFRs described in this section are added to the Security Target in order to support the optional H/W Authentication, which may be used to exit Restricted Mode when implemented. These SFRS directly support OT.Restricted_Mode, the rationale is given in the table below.

[54] [selection: *Triple-DES, AES or other approved algorithms]*]

[55] [selection: *change_default, query, modify, delete, clear]*[assignment: *other operations*]

[56] [assignment:*list of TSF Data*

[57] [assignment:*the authorised identified roles*

[58] [selection: *SHA-1 or other approved algorithms]*]

[59] [assignment:*cryptographic keysizes*

[60] [selection:*FIPS 180-2 or other approved standards*]

Table 27. Additional Security Functional Requirements defined for the TOE

SFR	Rationale
FDP_ACC.2/RM	Contributes to the coverage of the objective by defining the subject of the Restricted Mode access control SFP.
FDP_ACF.1/RM	Contributes to cover the objective by controlling access to objects for all operations.
FMT_MSA.1/RM	Management of security attributes (Restricted Mode)
FMT_SMF.1/RM	Contributes to cover the objective by defining the management functions of the restricted mode.
FMT_SMR.1/RM	Contributes to cover the objective by defining the security role *S.HWAuth*
FIA_UAU.1/RM	Contributes to cover the objective by requiring authentication before resetting the Attack Counter.
FIA_UID.1/RM	Contributes to cover the objective by requiring identification before resetting the Attack Counter.

6.1.6.1 FDP_ACC.2/RM

FDP_ACC.2/RM **Complete Access Control (RM)**

Hierarchical to: FDP_ACC.1

Dependencies: FDP_ACF.1 Security Attribute based Access Control

FDP_ACC.2.1/RM The TSF shall enforce the *Restricted Mode Access Control SFP* [61] on *S.HWAuth* [62] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/RM The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

6.1.6.2 FDP_ACF.1/RM

FDP_ACF.1/RM **Security attribute based access control(RM)**

Hierarchical to: No Other Components

Dependencies:

FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1/RM The TSF shall enforce the *Restricted Mode Access Control Policy* [63]] to objects based on the following: **S.HWAuth - ATTACK_COUNTER** [64] .

FDP_ACF.1.2/RM The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *The ATTACK_COUNTER is reset by S.HWAuth completing H/W Authentication* [65].

[61] [assignment:*access control SFP*]

[62] [assignment: *list of subjects and objects*]

[63] [assignment:*access control SFP*]

[64] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

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

FDP_ACF.1.3/RM The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none]* [66].

FDP_ACF.1.4/RM The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *Deny all operations on all objects if the ATTACK_COUNTER has reached its limit (restricted mode), except for operations listed in FMT_SMF.1[RM]* [67] .

6.1.6.3 FMT_MSA.1/RM

FMT_MSA.1/RM **Management of Security Attributes**

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/RM The TSF shall enforce the *Hardware Authentication Access Control SFP* [68] to restrict the ability to *modify* [69] the security attributes *Attack Counter* [70] to *S.HWAuth* [71].

6.1.6.4 FMT_SMF.1/RM

FMT_SMF.1/RM **Specification of Management Functions (RM)**

Hierarchical to: No Other Components

Dependencies: No dependencies.

FMT_SMF.1.1/RM The TSF shall be capable of performing the following management functions: [72]

6.1.6.5 FMT_SMR.1/RM

FMT_SMR.1/RM **Security Roles (RM)**

Hierarchical to: No Other Components

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1/RM The TSF shall maintain the roles *S.HWAuth* [73].

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

6.1.6.6 FIA_UAU.1/RM

FIA_UAU.1/RM **Timing of authentication (RM)**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1/RM The TSF shall allow

[66] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[67] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[68] [assignment:*access control SFP(s), information flow control SFP(s)*]
[69] [selection:*change_default, query, modify, delete, [assignment: other operations*]
[70] [assignment:*list of security attributes*]
[71] [assignment:*the authorised identified roles*]
[72] [assignment:*list of management functions to be provided by the TSF*]
[73] [assignment:*the authorised identified roles*]

1. *Reset the card*
2. *H/W Authentication Mechanism based on AES*

[74] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/RM The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.6.7 FIA_UID.1/RM

FIA_UID.1/RM **Timing of Authentication**

Hierarchical to: No other components.

Dependencies: No other Dependencies

FIA_UID.1.1/RM The TSF shall allow:

1. *Reset the card*
2. *Hardware Authentication based on AES*

[75] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/RM The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.7 SFR dependency Analysis

The Security Target SFR dependencies concur with the analysis provided in Section 6.3.2 of the Protection Profile [7]

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

Table 28. SFR Dependency Analysis

SFR	Dependencies	Satisfied by
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_SMF.1	FMT_SMR.1 FMT_SMF.1
FDP_ACC.2/RM	FDP_ACF.1	FDP_ACF.1/RM
FDP_ACF.1/RM	FDP_ACC.1 FMT_MSA.3	unsupported unsupported

[74] [assignment:*list of TSF mediated actions*]

[75] [assignment:*list of TSF mediated actions*]

SFR	Dependencies	Satisfied by
FMT_MSA.1/RM	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/RM FMT_SMR.1/RM FMT_SMF.1/RM
FMT_SMF.1/RM	No Dependencies	No Dependencies
FMT_SMR.1	FIA_UID.1	FIA_UID.1/RM
FIA_UID.1/RM	FIA_UAU.1	FIA_UAU.1/RM
FIA_UAU.1/RM	No Dependencies	No Dependencies

The rationale for unsupported dependencies is given below

Table 29. 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.
FDP_ACF.1/RM	The access control TSF according to FDP_ACF.1/RM uses security attributes (Attack Counter Initial Value) which are defined during the personalisation and are fixed over the whole life time of the TOE. No management of this security attribute (i.e. FMT_SMF.1 or FMT_MSA.3) is necessary here.

6.2 Security Assurance Requirements for the TOE

TOE Security Assurance Requirements stated in section 6.2 of the claimed PP0056 [7] are those taken from the Evaluation Assurance Level 5 (EAL5) augmented by ALC_DVS.2, ALC_FLR.1 and AVA_VAN.5

This Security Target makes the claim for Evaluation Assurance Level 5 (EAL5) augmented by

- ALC_DVS.2
- ALC_FLR.1
- AVA_VAN.5

6.3 Security Requirements Rationale

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

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/PACE) and data communication required are satisfied. Accesses are recorded via FAU_SAS.1

The function includes control over the Terminal gaining access to MRTD's chip data (FDP_ACC.1/TRM, FDP_ACF.1/TRM) 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:
  - Create, Write and Read EF.COM, EF.SOD, EF.DG1 to EF.DG16
  - Create, import and generate initial Active Authentication Private Key (FMT_MTD.1/AAPK)
  - Create, import and generate initial Chip Authentication Private Key (FMT_MTD.1/CAPK)
  - Write initial Country Verifying Certification Authority Public Key (FMT_MTD.1/CVCA_INI
  - Write initial Country Verifying Certification Authority Certificate (FMT_MTD.1/CVCA_INI)
  - Write initial SO_D by Initialization Agent (FMT_MTD.1/PA)
  - Write initial current Date (FMT_MTD.1/CVCA_INI)
  - 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 authorization of Extended Inspection System during Usage Phase 4 to:
  - Read EF.DG3 (Fingerprint)
  - Read EF.DG4 (Iris)
  - Update Current Date (FMT_MTD.1/DATE)
- Control over the authorization of CVCA during usage Phase 4 to:
  - Update Country Verifying Certification Authority Public Key (FMT_MTD.1/CVCA_UPD)
  - Update Country Verifying Certification Authority Certificate (FMT_MTD.1/CVCA_UPD)
  - Update current date (FMT_MTD.1/CVCA_UPD)
- Control over the Terminal during Usage Phase 4 to:
  - Read EF.DG1, EF.DG2, EF.DG5 to EF.DG16
  - Update Current Date when Terminal is a Document Verifier (FMT_MTD.1/DATE)
  - Create new Active Authentication Keys (FMT_MTD.1/AAPK)
  - Prevent reading EF.DG3, even when Terminal is authenticated as CVCA or DV
  - Prevent reading EF.DG4, even when Terminal is authenticated as CVCA or DV

  - Prevent reading Document Basic Access Keys, Active Authentication Private Key, Personalisation Agent Keys (FMT_MTD.1/KEY_READ)
  - Prevent modification of EF.DG.1 to EF.DG16
- 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 Chip Authentication (FDP_UCT.1/TRM, FDP_UIT.1/TRM)

This security functionality covers:

- FAU_SAS.1
- FDP_ACC.1/TRM
- FDP_ACF.1/TRM
- FDP_UCT.1/TRM
- FDP_UIT.1/TRM
- FMT_MTD.1/INI_ENA
- FMT_MTD.1/CVCA_INI
- FMT_MTD.1/CVCA_UPD
- FMT_MTD.1/DATE
- FMT_MTD.1/CAPK
- FMT_MTD.1/AAPK
- FMT_MTD.1/PA
- FMT_MTD.1/KEY_READ

7.2 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). This includes disabling read access to Initialization data at completion of the personalization phase (FMT_SMF.1).

This security functionality covers:

- FMT_SMF.1

7.3 SF.Personalizer Authentication

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

The authentication requires a symmetric encryption using TDES in CBC mode with a key length of 112 bits (FCS_COP.1/PACE_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_EMS.1).

This security functionality covers:

- FIA_UAU.5/PACE
- FIA_UAU.1/PACE
- FIA_UID.1/PACE
- FCS_COP.1/PACE_ENC
- FPT_EMS.1

7.4 SF.PACE

The Basic Access System and the travel document mutually authenticate by means of a Basic Access Control mechanism (FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.5/PACE) with challenge number exchange and verification. This random number (challenge) will be enciphered with the secret symmetric key by the receiver and then will be verified by the sender. This security service manages the session keys exchanged between the terminal and the TOE and provides the means to identify and authenticate the users in a secure way. The algorithm used for encryption/decryption is a Triple-DES in CBC mode with key sizes 112 bits (FCS_COP.1/PACE_ENC), while the message authentication code is computed according to Retail MAC algorithm and cryptographic key sizes 112 bit (FCS_COP.1/PACE_MAC). These authentication keys are derived by the SHA-1 algorithm. After a successful BAC authentication, the Basic Access System is able to read less sensitive data, such as the MRZ, the facial image and other data easily available from other sources.

The PACE-enabled Basic Access System and the travel document mutually authenticate by means of a PACE V2 protocol (FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.5/PACE).

The travel document and the Inspection System perform a Diffie-Hellman (DH or ECDH) key agreement by means of keys derived from MRZ or CAN. After a successful authentication, the generated session keys are independent of MRZ or CAN entropy. This security service manages the session keys exchanged between the terminal and the TOE and provides the means to identify and authenticate the users in a secure way. The algorithm used for secure messaging encryption/decryption may be either a 3DES or AES (FCS_COP.1/PACE_ENC), the MAC algorithm may be a Retail MAC, coupled with 3DES encryption, or CMAC, coupled with AES encryption (FCS_COP.1/PACE_MAC).

After a successful PACE V2 authentication, the Inspection System is able to read less sensitive data, such as the MRZ, the facial image and other data easily available from other sources.

If passport inspection is performed on a Basic Inspection System, the travel document’s authenticity may be proved executing the Active Authentication protocol. The use of challenges enforces a protection against replay (FIA_UAU.4/PACE).

This security functionality covers:

- FIA_AFL.1/PACE
- FIA_UID.1/PACE
- FIA_UAU.1/PACE
- FIA_UAU.4/PACE
- FIA_UAU.5/PACE
- FCS_COP.1/PACE_ENC
- FCS_COP.1/PACE_MAC
- FPT_EMS.1

7.5 SF.Terminal Authentication

This TSF provides Terminal Authentication to allow the TOE to authenticate the terminal using the public authentication material that is presented during the Chip Authentication protocol (DH or ECDH), enforcing the Secure Messaging session that was then open (FIA_UAU.1, FIA_UAU.5).

Terminal Authentication is a two move challenge-response protocol that provides explicit unilateral authentication of the inspection system. The terminal Authentication protocol requires that the card validates the chain of certificates sent by the inspection system (Terminal) (FMT_MTD.3). Certificate validation corresponds to a signature verification (FCS_COP.1/SIG_VER) requiring Hash calculation (FCS_COP.1/SHA). A successful sequence of certificates validation (CVCA-DV-IS) completes the terminal authentication.

The protocol involves the CVCA public key stored on the chip and a nonce, generated by the TOE (FCS_RND.1). The use of challenges enforces a protection against replay (FIA_UAU.4).

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/AA). 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 ICAO DOC 9303 [10].

This TSF involves an optional asymmetric Key Pair (K_{PrAA}, K_{PuAA}) which the public part of,K_{PuAA}, is stored in DG15 and private part, K_{PrAA} is stored securely within the chip.

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 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_EMS.1).

This security functionality covers:

- FIA_API.1/AA
- FCS_RND.1
- FCS_COP.1/SHA
- FCS_COP.1/SIG_GEN
- FIA_UAU.4/AA
- FPT_EMS.1

7.7 SF.Chip Authentication

This TSF provides the Chip Authentication protocol to allow the Extended Inspection System to authenticate the TOE (FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.5/ PACE, FCS_CKM.1/CA). This authentication mechanism involves the Chip Authentication Key Pair: Diffie-Hellman Public Key PK_{PICC} and Private Key SK_{PICC}.

The public key is stored in EF.DG14 and available to any Terminal wishing to perform Chip Authentication (FIA_API.1/CAP). This protocol requires that a shared secret is calculated by both the inspection system and the MRTD's chip. The MRTD's chip exports its static Diffie-Hellman Public Key, and the inspection system imports an ephemeral public key that will help the MRTD’s chip to compute the shared secret. This computation requires a hash computation (FCS_COP.1/SHA) and a Diffie-Hellman key derivation (FCS_CKM.1/CA).

Completion of the Chip Authentication protocol means that the Secure Messaging session started with BAC is updated: the session keys ($K_{ENC}$and K_{MAC}) are derived from the shared secret. All further communication with the TOE is handled by SF.Secure Messaging Security Function, enforcing confidentiality and integrity over transferred data (FIA_UAU.5/PACE).

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_EMS.1).

This security functionality covers:

- FCS_CKM.1/CA
- FIA_UAU.1/PACE
- FIA_UAU.4/PACE
- FIA_UAU.5/PACE
- FIA_API.1
- FPT_EMS.1

7.8 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/PACE, FIA_UAU.5/PACE): 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 (FTP_ITC.1). The secure communication channels are enforced by cryptographic functions.

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

- Confidentiality is ensured by a TDES (FCS_COP.1/CA_ENC) or AES(FCS_COP.1/PACE_ENC) encryption
- Integrity is achieved by calculation, embodiment and verification of a Retail MAC or CMAC (FCS_COP.1/PACE_MAC or FCS_CA_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 Chip Authentication protocol is required after termination of a Secure Messaging session (FIA_UAU.6/PACE and FIA_UAU.6/EAC).

Encryption operations are protected against DPA/SPA, timing attacks, and electromagnetic emanation (FPT_EMS.1), by the certified Cryptogrphic Library.

This security functionality covers:

- FCS_CKM.4
- FCS_COP.1/CA_ENC
- FCS_COP.1/CA_MAC
- FCS_COP.1/PACE_ENC

- FCS_COP.1/PACE_MAC
- FIA_UAU.1/PACE
- FIA_UAU.4/PACE
- FIA_UAU.5/PACE
- FIA_UAU.6/PACE
- FIA_UAU.6/EAC
- FDP_UCT.1/TRM
- FDP_UIT.1/TRM
- FPT_EMS.1
- FTP_ITC.1

7.9 SF.Crypto

This Security Function is responsible for providing cryptographic support to all the other Security Functions including :

- Data hashing using SHA1, SHA224, SHA256, SHA384, SHA512. (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)
- ECDSA Signature Verification with ECC Keys of length 192, 224, 256, 384, 521 bits
- TDES 2 Keys and 3 Keys in CBC and ECB modes for PACE and Chip Authentication (FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC)
- AES for PACE (FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC)
- 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).
- MAC is generated and verified using TDES with 2 or 3 keys
- Diffie-Hellman calculations for DH and ECDH based protocols

This TSF enforces protection of Key material during cryptographic processing against state-of-the-art attacks (FPT_EMS.1)

This security functionality covers:

- FCS_CKM.1/CA
- FCS_CKM.1/DH_PACE
- FCS_CKM.4
- FCS_COP.1/CA_ENC
- FCS_COP.1/CA_MAC
- FCS_COP.1/PACE_ENC
- FCS_COP.1/PACE_MAC
- FCS_COP.1/SIG_GEN
- FCS_COP.1/SIG_VER
- FCS_COP.1/SHA
- FCS_RND.1
- FCS_EMS.1

7.10 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 RNG at each power-up (FPT_TST.1)
- Deleting authentication resources (Biometrics data, 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.
- Initializing memory after reset (FDP_RIP.1)
- Initializing memory of de-allocated data (FDP_RIP.1)
- Preserving secure state after sensitive processing failure or potential physical tampering or intrusion detection (FPT_FLS.1, FPT_PHP.3)
- 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)
- Introducing managed time delay penalty to failed PACE authentications (FIA_FLT.1/PACE)

This security functionality covers:

- FCS_CKM.4
- FDP_RIP.1
- FIA_AFL.1/PACE
- FMT_LIM.1
- FMT_LIM.2
- FPT_FLS.1
- FPT_PHP.3
- FPT_TST.1

7.11 SF.RM

SF.RM provides a restricted mode that is entered when the Attack Counter reaches its limit. In restricted mode only limited functionality is available. Only the S.HWAuth is able to reset the Counter to leave the restricted mode. This supports FDP_ACC.2[RM], FDP_ACF.1[RM], FMT_MSA.3[RM], FMT_MSA.1[RM], and FMT_SMF.1[RM]. SF.RM only allows a limited set of operations to not identified and not authenticated users when in restricted mode. All other operations require identification and authentication (FIA_UID.1[RM], FIA_UAU.1[RM]).

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_EMS.1).

This security functionality covers:

- FDP_ACC.2/RM
- FDP_ACF.1/RM
- FMT_MSA.1/RM
- FMT_MSA.3/RM
- FIA_UID.1/RM

- FIA_UAU.1/RM

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”, Extended Access Control with PACE (EAC PP), certified under the reference BSI-CC-PP-0056-V2-2012-MA-02, Version 1.3.2.

[8] Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), certified under the reference BSI-CC-PP-0068-V2-2011-MA-01, Version 1.01.

[9] 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.

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

[11] ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.1, April 2014.

[12] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token; February 2015.

8.2 Developer documents

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

[14] SmartePP ICAO Personalization guide; Revision 1.4, 09 December 2020 .

[15] 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

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

[17] 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.

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

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

8.4 Standards referenced in ICAO

[20] PKCS #3 Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, November 1, 1993

[21] TR-03111 Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline; Elliptic Curve Cryptography, v1.11 17.04.2009

[22] TR-03110-EAC Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), October 2010

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

Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

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-EAC