

# Security Target Lite EP-COS V3.0

## NSCIB-CC-15-87206

NXP Semiconductors Germany GmbH, Business Unit  
Security and Connectivity

Rev. 2.0 — 28 February 2017  
361620

### Document information

Info	Content
<b>Keywords</b>	ASE, EP-COS, Common Criteria, EAL4 augmented, Security Target Lite
<b>Abstract</b>	This document contains information to fulfill the requirements of the Common Criteria component ASE (Security Target) for the Evaluation of the EP-COS V3.0 developed and provided by NXP Semiconductors, Business Unit Security & Connectivity, according to the Common Criteria for Information Technology Security Evaluation Version 3.1 R4 at EAL4 augmented.



## Revision history

Rev	Date	Description
2.0	20170228	Security Target Lite derived from the complete Security Target version 2.0

## Contact information

For more information, please visit: <http://www.nxp.com>

## 1. ST Introduction

### 1.1 ST Reference

Title:	Security Target Lite EP-COS V3.0
Document version:	Rev. 2.0
Date of document:	28 February 2017
TOE reference:	EP-COS V3.0
Certification ID:	NSCIB-CC-15-87206
Sponsor of the evaluation:	NXP Semiconductors Germany GmbH, Business Unit Security and Connectivity
Developer of security IC and crypto library:	NXP Semiconductors Germany GmbH, Business Unit Security and Connectivity
Developer of embedded software (operating system) and object system:	Subcontractor of NXP

### 1.2 TOE Overview

The Security Target Lite EP-COS V3.0 defines the TOE, the conformance claim, the security problem definition, security objectives, security requirements and TOE summary specification for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO) and conformant to the Protection Profile BSI-CC-PP-0055 [19]. It addresses the advanced security methods Basic Access Control in the 'ICAO Doc 9303' [8] and optional Active Authentication as described in [11] if enabled by loading the Active Authentication key pair during personalization.

### 1.3 TOE Definition

#### TOE Description

The Target of Evaluation (TOE) EP-COS V3.0 is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to 'ICAO Doc 9303' [8] as well as optional Active Authentication as described in [11] if enabled during the personalization by loading the Active Authentication key pair.

The TOE comprises of

1. the circuitry of the MRTD's chip P60D081PVB (P6021yVB configuration) with Crypto Library V3.1.2 on P60D081PVB
2. the IC Embedded Software (operating system),
3. the MRTD application BAC with AA V2.0 and
4. the associated guidance documentation Personalization Guidance (AGD\_PRE) EP-COS\_V3.0, Version 0.96 and Operational User Guidance (AGD\_OPE) EP-COS V3.0, Version 0.96.

The circuitry of the MRTD's chip P60D081PVB is certified under certificate identification BSI-DSZ-CC-0955 and the Crypto Library V3.1.2 on P60D081PVB is certified under certificate identification NSCIB-CC-15-66030.

The physical boundaries of the TOE are the inlay embedding the P60D081PVB and the visual readable data including -but not limited to- personal data of the MRTD holder as detailed in [19]. The TOE comprises a contactless interface that supports the communication according to the ISO/IEC 14443 Standard.

The logical boundaries of the TOE comprise the command set supported by the operating system and the MRTD application. This command set allows controlled access to the personal data (logical MRDT) as described in [19].

### TOE usage and security features for operational use

The MRTD issued by a state or organization is used by the holder as described in the Protection Profile [19]. The following TOE security functionality is most relevant during the operational use:

- Self-protection of the TOE and the data stored on the TOE
- The Basic Access Control authorizes the terminal to read the logical MRTD after optical read of the MRTD
- Protection of the communication channel between the terminal and the TOE regarding authenticity, integrity and confidentiality
- Preventing inconspicuous identification or tracking of a MRTD.
- Optional Active Authentication to verify the authenticity of the Chip if enabled during personalization by loading an Active Authentication key pair.

The protection is provided as described in [19].

### TOE life cycle

The TOE life cycle is described in terms of the four life cycle phases in [19]. With respect to [18], these TOE life-cycle phases are further subdivided into 7 phases. The following description provides the mapping between these two life cycle descriptions.

#### Phase 1 "Development"

(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

(Step2) The 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 IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories (ROM) is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the MRTD application and the guidance documentation is securely delivered to the MRTD manufacturer.

The life cycle phase 1 (step1) related to development of the integrated circuit is part of the evaluation of the underlying hardware platform, refer also to [18]. The software development in phase 1 (step2) using the IC guidance documentation including the secure delivery of software and data to the IC Manufacturer are in the scope of the

evaluation. The delivery comprises the IC Embedded Software stored in ROM as well as software (software extensions and patches) and data (FabKey including Personalization agent authentication key and pre-personalization data) to be stored in the non-volatile memory during wafer testing.

#### Phase 2 “Manufacturing”

(Step3) In a first step 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 memory (ROM). The IC manufacturer writes the IC Identification Data and the pre-personalization 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 manufacture to the MRTD manufacturer.

Complements of the Security IC Embedded Software as well as FabKey including Personalization agent authentication key and pre-personalization data are delivered to the IC manufactures in phase 1 as described above. The IC manufacturer provides functionality to store these deliverables in the non-volatile programmable memories (EEPROM) of each MRTD chip during wafer testing as described in [20].

(Step4) The module with the hardware IC and the antenna are assembled as inlay for the passport book.

(Step5) The creation of the MRTD application is performed together with step 6 in phase 3. The Pre-personalization Data is already loaded in step 3.

The inlay together with the IC Identifier is securely delivered from the IC manufacturer to the MRTD manufacturer. The MRTD manufacturer is also the Personalization Agent. The MRTD developer provides the relevant parts of the guidance documentation to the Personalization Agent.

The TOE is delivered by the IC manufactures to the Personalization Agent. The production and testing of the hardware platform including the assembly steps up to the inlay are subject of the evaluation of the underlying hardware platform, refer to [18] and [20].

Using application note 1 the creation of the MF and the ICAO.DF is done by the Personalization Agent.

#### Phase 3 “Personalization of the MRTD”

(Step6) The personalization of the MRTD includes the steps as described in [19].

The signing of the Document security object by the Document Signer [8] 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.

The Personalization Agent equips the MRTD's chip with the Active Authentication key pair during the personalization to enable the Active Authentication for the MRTD. If the MRTD does not store an Active Authentication key pair the Active Authentication is disabled.

Using application note 2, the TSF data comprise (but are not limited to) the Personalization Agent Authentication Key(s), the Basic Authentication Control Key and optionally the Active Authentication key pair.

Using application note 3, the Personalization Agent will perform the personalization.

#### Phase 4 “Operational Use”

(Step7) The TOE is used as MRTD chip by the traveler and the inspection systems in the “Operational Use” phase. The user data can be read according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State but they can never be modified.

Using application note 4, the authorized Personalization Agent is not able to update or add data in the MRTD application during the operational usage phase.

Using application note 5: Phase 1, step 2 is part of the evaluation. Phase 2 up to step 4 is covered by the evaluation of the underlying hardware platform.

#### **Non-TOE hardware/software/firmware required by the TOE**

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.

## 2. Conformance Claims

### 2.1 CC Conformance Claim

This Security Target Lite EP-COS V3.0 claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012, [\[1\]](#)
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012, [\[2\]](#)
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012, [\[3\]](#)

as follows

- Part 2 extended,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012, [\[4\]](#)

has to be taken into account.

### 2.2 PP Claim

This Security Target Lite EP-COS V3.0 claims strict conformance to the Protection Profile Machine Readable Travel Document with „ICAO Application“, Basic Access Control, BSI-CC-PP-0055 [\[19\]](#).

### 2.3 Package Claim

This Security Target Lite EP-COS V3.0 is conforming to assurance package EAL4 augmented with ALC\_DVS.2 and ATE\_DPT.2 defined in CC part 3 [\[3\]](#).

### 2.4 Conformance Rationale

The Security Target Lite EP-COS V3.0 contains all assumptions, organizational security policies, threats, security objective for the TOE, all security objectives for the operational environment, security functional requirements and assurance requirements as defined in the protection profile BSI-CC-PP-0055.

Note that the description of the logical MRTD in the protection profile BSI-CC-PP-0055 addresses all data groups as defined in [\[8\]](#). The specification includes a number of optional and conditional data groups, only DG1 and DG2 are required. The TOE supports the required DG1, DG2 as well as the optional DG11, DG12 and DG13. In addition the conditional DG15 is supported in case Active Authentication is enabled. The data groups DG3 and DG4 shall only be supported, if the MRTD supports extended access control. DG5 to DG10 are optional, DG14 is conditional and stores additional security infos relevant for extended access control and DG16 is also optional.

Note the modification of the Organizational Security Policies "P.Manufact". The Personalization Agent Key for authentication is already loaded by the IC Manufacturer to support not only unique identification but also transport protection to the personalization agent. Since the MRTD Manufacturer is also considered to be the personalization agent and the creation of the MRTD application and the personalization are performed at the same time and in the same secure environment, the protection of the TOE between creation and personalization is given. The modification of "P.Manufact" has no impact on the rationale in the PP. Only the Personalization Agent Key is explicitly mentioned as pre-personalization data for the transport protection between creation of the MRTD and personalization of the MRTD. Since these two steps are performed together and the loading of the Personalization Agent Key extends the protection to the delivery between IC Manufacturer and personalization agent, the strict conformance of the Security Target is maintained.

The SFR short family name FPT\_EMSEC and the short component name FPT\_EMSEC.1 defined in BSI-CC-PP-0055 are changed to FPT\_EMS respective FPT\_EMS.1 in order to meet [\[3\]](#) ASE\_ECD.1.4C (i.e. 3 letters for the short family identification). In addition the private Active Authentication key is added part of the confidential TSF data.

The components FDP\_ACC.1 and FDP\_ACF.1 defined in the protection profile BSI-CC-PP-0055 are renamed in FDP\_ACC.1/BAC and FDP\_ACF.1/BAC because the component FDP\_ACC.1 and FDP\_ACF.1 are iterated in order to include FDP\_ACC.1/AA and FDP\_ACF.1/AA with a dedicated access control policy for the Active Authentication key pair. The iteration of FCS\_COP.1/AA is added to include the optional cryptographic operations performed with the Active Authentication key. FIA\_API.1 is included to model the authentication using the Active Authentication key and FMT\_SMF.1 is extended to include the enabling and disabling of the Active Authentication in the management functions. In addition, FMT\_MTD.1/KEY\_WRITE and FMT\_MTD.1/KEY\_READ for the management of TSF data are extended to include the management of the Active Authentication key.

The Security Target Lite EP-COS V3.0 adds the threat T.Counterfeit covered by the security objective for the TOE OT.Active\_Auth\_Proof requiring the TOE to support additional security functionality Active Authentication. The security objectives for the operational environment are only dealing with Active Authentication: (1) OE.Active\_Auth\_Prep addressing enabling or disabling Active Authentication and by loading the Active Authentication Key Pair if enabling is chosen, and (2) OE.Active\_Auth\_Verif addressing the usage of Active Authentication by Basic Inspection Systems if Active Authentication is enabled for the TOE. The OT.Active\_Auth\_Proof is covered by the additional security functional requirements FCS\_COP.1/AA and FIA\_API.1 and SFR FDP\_ACC.1/AA, FDP\_ACF.1/AA. The FMT\_SMF.1 of the BSI-CC-PP-0055 is extended in order to identify enabling and disabling of Active Authentication in the Personalization Phase as management of TSF. FMT\_MTD.1/KEY\_WRITE is extended because the Active Authentication key pair must be managed in the same way as the Document Basic Access Keys. FMT\_MTD.1/KEY\_READ is extended because the restrictions for the Document Basic Access Keys also apply for the private component of the Active Authentication key pair. The assumption A.AA-Key Pair is added since the Active Authentication key is generated in the Personalization environment and not by the MRTD chip. The assumption is limited to the Active Authentication key pair that must be controlled by the environment.



Note that the Protection Profile [19] refers to the Protection Profile “Security IC Platform, BSI-PP-0035-2007, Version 1.0, June 2007” that is superseded by the Protection Profile [18]. The substitution is discussed where required. The strict conformance claim is still applicable because the main parts including security problem definition, security objectives and security functional requirements of BSI-PP-0035-2007 are taken over by the BSI-PP-0084-2014.

## 3. Security Problem Definition

### 3.1 Introduction

#### Assets

The Security Target Lite EP-COS V3.0 claims strict conformance to the Protection Profile [19] and the definition of assets as included in [19] is valid for this Security Target Lite EP-COS V3.0. Since the TOE supports active authentication optionally the related Active Authentication Key Pair is also an asset if configured.

The TOE does not store and support all data groups defined in the Protection Profile [19]. The TOE supports the following data groups: EF.COM, EF.SOD, EF.DG1, EF.DG2, EF.DG11 to EF.DG13 and optional EF.DG15. The rationale is provided in section 2.4.

The description in [19] also covers the subjects that are supplemented here with TOE specific remarks.

- The Personalization Agent role is gained by users after authentication by means of the Symmetric Authentication Mechanism with the Personalization Agent Key.

Using application note 6, the Basic Inspection System role is gained by users after authentication by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. The TOE only distinguishes between the BIS and GIS as well as EIS in case the active authentication is enabled. The Terminal Authentication Protocol is outside the scope of this evaluation.

Using application note 7, an impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged MRTD. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

### 3.2 Assumptions

The Security Target Lite EP-COS V3.0 claims strict conformance to the Protection Profile [19] and the assumptions defined in [19] are valid for this Security Target Lite EP-COS V3.0.

The assumptions included in the Protection Profile [19].

#### **A.MRTD\_Manufact** MRTD manufacturing on steps 4 to 6

Details of the assumption are not repeated here. The assumption is addressed by ALC\_DVS.2 for the steps of the life cycle covered in the evaluation. For the remaining life cycle steps this is addressed in the Guidance for the Personalization Agent.

#### **A.MRTD\_Delivery** MRTD delivery during steps 4 to 6

Details of the assumption are not repeated here. The physical TOE is delivered from the IC manufacturer to the Personalization Agent and the evaluated delivery procedure of the hardware platform applies. Further on the Personalization Agent authentication key is exchanged between the MRTD developer and the Personalization Agent. This is addressed in the Guidance for the Personalization Agent.

#### **A.Pers\_Agent** Personalization of the MRTD's chip

Details of the assumption are not repeated here, it applies as defined in the Protection Profile [19].

**A.Insp\_Sys Inspection Systems for global interoperability**

Details of the assumption are not repeated here, it applies as defined in the Protection Profile [\[19\]](#).

Using application note 8, the support of the Passive Authentication mechanism is mandatory whereas the Basic Access Control is optional according to [\[8\]](#). This Security Target Lite EP-COS V3.0 does not address Primary Inspection Systems therefore the BAC is mandatory enforced by the TOE.

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

Details of the assumption are not repeated here, it applies as defined in the Protection Profile [\[19\]](#).

Application Note 9 does not include any option therefore it is applicable as described in [\[19\]](#).

The following assumption is added to cover the optional Active Authentication during the Personalization including the key generation.

**A.AA-Key Pair Cryptographic quality of the Active Authentication Key Pair**

The Personalization Agent ensures the generation of cryptographic strong and correct active authentication key pairs and the correct storage of the active authentication key pair on the TOE if active authentication is enabled.

**3.3 Threats**

The Security Target Lite EP-COS V3.0 claims strict conformance to the Protection Profile [\[19\]](#) and the threats defined in [\[19\]](#) are valid with the same conditions for this Security Target Lite EP-COS V3.0. The list of threats is included as they are applicable without any changes compared to [\[19\]](#).

<b>T.Chip_ID</b>	<b>Identification of MRTD's chip</b>
<b>T.Skimming</b>	<b>Skimming the logical MRTD</b>
<b>T.Eavesdropping</b>	<b>Eavesdropping to the communication between TOE and inspection system</b>
<b>T.Forgery</b>	<b>Forgery of data on MRTD's chip</b>
<b>T.Abuse-Func</b>	<b>Abuse of Functionality</b>
<b>T.Information_Leakage</b>	<b>Information Leakage from MRTD's chip</b>
<b>T.Phys-Tamper</b>	<b>Physical Tampering</b>
<b>T.Malfunction</b>	<b>Malfunction due to Environmental Stress</b>

The Security Target Lite EP-COS V3.0 includes one additional threat compared to the Protection Profile [\[19\]](#).

**T.Counterfeit Counterfeit of travel document chip**

Adverse action: An attacker with enhanced-basic attack potential produces an unauthorized copy or reproduction of a genuine travel document's chip to be used as part of a counterfeit travel document. This violates the authenticity of the travel document's chip used for authentication of a traveler by possession of a travel document.

The attacker may generate a new data set or extract completely or partially the data from a genuine travel document's chip and copy them to another appropriate chip to imitate this genuine travel document's chip.

Threat agent: having enhanced-basic attack potential, being in possession of one or more legitimate travel documents

Asset: authenticity of logical travel document data

Note that the threat T.Counterfeit is only averted by the TOE if the Active Authentication is enabled.

### 3.4 Organizational Security Policies

The Security Target Lite EP-COS V3.0 claims strict conformance to the Protection Profile [\[19\]](#) and the organizational security policies defined in [\[19\]](#) are valid for this Security Target Lite EP-COS V3.0. Therefore they are only listed.

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

The Initialization Data and the Pre-personalization Data which contains at least the Personalization Agent Authentication Key and the Unique Identification Number are written by the IC Manufacturer to identify the IC uniquely.

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

#### **P.Personal\_Data**      **Personal data protection policy**

Application Note 10 does not include any option therefore it is applicable as described in [\[19\]](#).

Note that the Organizational Security Policies "P.Manufact" is modified. The strict conformance of this Security Target is maintained according to the rationale in section 2.4.

## 4. Security Objectives

The Security Target Lite EP-COS V3.0 claims strict conformance to the Protection Profile [\[19\]](#) and the security objectives defined in [\[19\]](#) are valid for this Security Target Lite EP-COS V3.0. All security objectives defined in the Protection Profile are included as list.

### 4.1 Security Objectives for the TOE

#### **OT.AC\_Pers                      Access Control for Personalization of logical MRTD**

Using application note 11 the data written during the Personalization for the MRTD holder cannot be changed after the personalization process is finalised. The TOE does not provide the optional capability to add data by the Personalization Agent during the "Operational Use" phase.

#### **OT.Data\_Int                      Integrity of personal data**

#### **OT.Data\_Conf                      Confidentiality of personal data**

Application Note 12 does not include any option therefore it is applicable as described in [\[19\]](#).

#### **OT.Identification                      Identification and Authentication of the TOE**

Application Note 13 does not include any option therefore it is applicable as described in [\[19\]](#).

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

#### **OT.Prot\_Abuse-Func                      Protection against Abuse of Functionality**

#### **OT.Prot\_Inf\_Leak                      Protection against Information Leakage**

Application Note 14 does not include any option therefore it is applicable as described in [\[19\]](#).

#### **OT.Prot\_Phys-Tamper                      Protection against Physical Tampering**

#### **OT.Prot\_Malfunction                      Protection against Malfunctions**

Application Note 14 does not include any option therefore it is applicable as described in [\[19\]](#).

The Security Target Lite EP-COS V3.0 includes one additional security objectives for the TOE compared to the Protection Profile [\[19\]](#).

#### **OT.Active\_Auth\_Proof                      Proof of MRTD's chip authenticity by means of Active Authentication**

The TOE must provide security functionality for Active Authentication Proof that allows the Basic Inspection Systems of the receiving State to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization if the Active Authentication Private Key is installed. The TOE must support the import of Active Authentication Key Pairs.

### 4.2 Security Objectives for the Operational Environment

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

<b>OE.MRTD_Manufact</b>	<b>Protection of the MRTD Manufacturing</b>
<b>OE.MRTD_Deliver</b>	<b>Protection of the MRTD delivery</b>
<b>OE.Personalization</b>	<b>Personalization of logical MRTD</b>
<b>OE.Pass_Auth_Sign</b>	<b>Authentication of logical MRTD by Signature</b>
<b>OE.BAC-Keys</b>	<b>Cryptographic quality of Basic Access Control Keys</b>

The Security Target Lite EP-COS V3.0 includes one additional security objectives for the Operational Environment compared to the Protection Profile [\[19\]](#). This will be implemented by the issuing State or Organization.

**OE.Active\_Auth\_Prep      Preparation of Active Authentication**

The Personalization Agent generates the MRTD's Active Authentication Key Pair outside the MRTD chip for load onto the MRTD chip and shall ensure (i) the cryptographic quality of the Active Authentication Key Pair and (ii) the secrecy of the MRTD's Active Authentication Private Key outside the TOE. The Personalization Agent enables Active Authentication by writing the Active Authentication Public Key in the EF.DG15 of the MRTD chip and signing the Document Security Object EF.DG15. If the Active Authentication is enabled for the MRTD chip the Personalization Agent shall ensure that the Active Authentication Public Key matches the Active Authentication Private Key written to the authentic MRTD chip. If Active Authentication is not to be enabled the Document Security Object EF.DG15 is signed with empty DG15.

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

<b>OE.Exam_MRTD</b>	<b>Examination of the MRTD passport book</b>
<b>OE.Passive_Auth_Verif</b>	<b>Verification by Passive Authentication</b>
<b>OE.Prot_Logical_MRTD</b>	<b>Protection of data from the logical MRTD</b>

The Security Target Lite EP-COS V3.0 includes one additional security objectives for the Operational Environment compared to the Protection Profile [\[19\]](#). This will be implemented by the receiving State or Organization.

**OE.Active\_Auth\_Verif      Verification of Active Authentication of MRTD chip**

The Basic Inspection Systems must have successfully verified the signature of Document Security Objects and the integrity of the not empty data element DG15 (Active Authentication Public Key) of the logical MRTD before running Active Authentication of the MRTD chip. If data element DG15 of the logical MRTD is empty the Active Authentication is not supported by the MRTD chip.

### 4.3 Security Objective Rationale

The following table provides an overview for security objectives coverage.

**Table 1. Security Objective Rationale**

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Active_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Active_Auth_Prep	OE.Personalization	OE.Pass_Auth_Sign	OE.Active_Auth_Verif	OE.BAC-Keys	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
T.Chip-ID				x												x			
T.Skimming			x													x			
T.Eavesdropping			x																
T.Forgery	x	x						x						x			x	x	
T.Counterfeit					x							x			x				
T.Abuse-Func						x							x						
T.Information_Leakage							x												
T.Phys-Tamper								x											
T.Malfunction									x										
P.Manufact				x															
P.Personalization	x			x									x						
P.Personal_Data		x	x																
A.MRTD_Manufact										x									
A.MRTD_Delivery											x								
A.Pers_Agent													x						
A.Insp_Sys																	x		x
A.BAC-Keys																x			
A.AA-Key Pair												x							

The detailed justification for the OSPs and the threats defined in the Protection Profile [19] is already provided in this Protection Profile. The extensions of the security problem added in this Security Target Lite EP-COS V3.0 do not impact the set of definitions included in the Protection Profile. Therefore the rationale included in the Protection Profile remains valid and is not reproduced here. In the following the rationale for the extensions is provided.

The threat **T.Counterfeit** “Counterfeit of travel document chip” addresses the undetected unauthorized copy or reproduction of a genuine travel document’s chip used as part of a counterfeit travel document. The security objective OT.Active\_Auth\_Proof “Proof of MRTD’s chip authenticity by means of Active Authentication” requires the TOE to provide the security functionality of import of the Active Authentication Key Pair and Active Authentication Proof if the Active Authentication Private Key is installed. The security objective for the issuing State OE.Active\_Auth\_Prep “Preparation of Active Authentication” describes key pair generation outside the TOE and enabling / disabling the Active Authentication for the TOE describes the configuration of the active authentication. OE.Active\_Auth\_Verif “Verification of Active Authentication of MRTD chip” describes the Verification of Active Authentication Verification by the Basic Inspection System if Active Authentication is enabled for the TOE.

The assumption A.AA-Key Pair "Cryptographic quality of the Active Authentication Key Pair" is covered by the security objective for the TOE environment OE.Active\_Auth\_Prep "Preparation of Active Authentication" including the generation and protection of the Active Authentication Key Pair when loaded by the Personalization Agent.



## 5. Extended Components Definition

This Security Target Lite EP-COS V3.0 uses components defined as extensions to CC part 2. Some of these components are defined in [18], other components are defined in this Security Target Lite EP-COS V3.0.

**Table 2. Extended Components Definition**

SFR	Initial Definition	Relation to [19]	Note
FAU_SAS.1	[18]	Definition not completely the same in [19]	The general assignment “ <i>list of subjects</i> ” is exchanged by “ <i>authorized user</i> ” and the assignment “ <i>type of persistent memory</i> ” is fixed to “ <i>audit records</i> ”. This is not considered to change the meaning or security functionality of the Security Functional Requirements.
FCS_RND.1	[19]	Specific	The component definition included in [19] is used.
FMT_LIM.1	[18]	Definition not completely the same in [19]	The policies regarding “limited availability” and “limited capability” are combined in [19] compared to [18]. This is not considered to change the meaning or security functionality of the Security Functional Requirements because their definition comprises the dependency between the two components.
FMT_LIM.2	[18]	Definition not completely the same in [19]	The policies regarding “limited availability” and “limited capability” are combined in [19] compared to [18]. This is not considered to change the meaning or security functionality of the Security Functional Requirements because their definition comprises the dependency between the two components.
FPT_EMS.1	[19]	Specific	Only name of the Security Functional Requirement is adapted, refer to section 2.4. Security Functional Requirement as defined in the PP [19].

### 5.1 Definition of the Family FIA\_API

To describe the IT security functional requirements of the TOE a functional family FIA\_API (Authentication Proof of Identity) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity by the TOE and enables the authentication verification by an external entity. The other families of the class FIA address the verification of the identity of an external entity by the TOE.

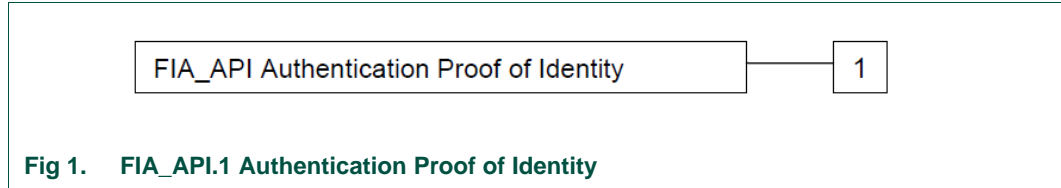
The other families of the Class FIA describe only the authentication verification of users’ identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA\_API in the style of the Common Criteria part 2 (cf. [3], chapter “Extended components definition (APE\_ECD)”) from a TOE point of view.

FIA\_API Authentication Proof of Identity

Family Behavior

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

Component leveling:



**Fig 1. FIA\_API.1 Authentication Proof of Identity**

FIA\_API.1 Authentication Proof of Identity, provides proof of the identity of the TOE, an object or an authorized user or role to an external entity.

Management FIA\_API.1  
 The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: FIA\_API.1  
 There are no actions defined to be auditable.

**FIA\_API.1 Authentication Proof of Identity**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA\_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [selection: *TOE*, [assignment: *object*, *authorized user or role*]] to an external entity.

## 6. Security Requirements

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph C.4 of Part 1 [1] of the CC. Each of these operations is used in this Security Target Lite EP-COS V3.0.

The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word “**refinement**” in bold text and the added/changed words are in bold text. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed. Additional security functional requirements dedicated to the optional Active Authentication and identified with “/AA”.

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the Security Target Lite EP-COS V3.0 authors are denoted as underlined text and the original text of the component is given by a footnote.

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the Security Target Lite EP-COS V3.0 authors are denoted by showing as underlined text and the original text of the component is given by a footnote.

The iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier.

Note that the application notes in chapter 6 of the Protection Profile [19] that request decisions from the ST writer are taken into account. Application notes providing more general guidance are also applicable for this Security Target Lite EP-COS V3.0 even if they are not repeated here.

The definition of the users “Manufacturer”, “Personalization Agent”, “Basic Inspection System” and “Terminal” used in the following chapter is given in section 3.1 of [19]. Note, that all these subjects are acting for homonymous users. All used objects are defined in section 6.1. The operations “write”, “read”, “modify”, and “disable read access” are used in accordance with the general linguistic usage. The operations “transmit”, “receive” and “authenticate” are originally taken from [2].

Definition of security attributes:

**Table 3. Definition of security attributes**

security attribute	values	meaning
terminal authentication status	none (Any Terminal)	default role (i.e. without authorization after start-up)
	Basic Inspection System	Terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2.
	Personalization Agent	Terminal is authenticated as Personalization Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2.

## 6.1 Security Functional Requirements for the TOE

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.

### 6.1.1 Class FAU Security Audit

The TOE shall meet the requirement “Audit storage (FAU\_SAS.1)” as specified below (Common Criteria Part 2 extended).

FAU\_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU\_SAS.1.1 The TSF shall provide the Manufacturer<sup>1</sup> with the capability to store the IC Identification Data<sup>2</sup> in the audit records.

### 6.1.2 Class Cryptographic Support (FCS)

The TOE shall meet the requirement “Cryptographic key generation (FCS\_CKM.1)” as specified below (Common Criteria Part 2).

FCS\_CKM.1 Cryptographic key generation – Generation of Document Basic Access Keys by the TOE

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/  
BAC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm<sup>3</sup> and specified cryptographic key sizes 112 bit<sup>4</sup> that meet the following: [8]. normative appendix 5<sup>5</sup>.

The TOE shall meet the requirement “Cryptographic key destruction (FCS\_CKM.4)” as specified below (Common Criteria Part 2).

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]

FCS\_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting with random data<sup>6</sup> that meets the following: none<sup>7</sup>.

<sup>1</sup> [assignment: *authorised users*]

<sup>2</sup> [assignment: *list of audit information*]

<sup>3</sup> [assignment: *cryptographic key generation algorithm*]

<sup>4</sup> [assignment: *cryptographic key sizes*]

<sup>5</sup> [assignment: *list of standards*]

<sup>6</sup> [assignment: *cryptographic key destruction method*]

<sup>7</sup> [assignment: *list of standards*]

## 6.1.2.1 Cryptographic operation (FCS\_COP.1)

The TOE shall meet the requirement “Cryptographic operation (FCS\_COP.1)” as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

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<sup>8</sup> in accordance with a specified cryptographic algorithm SHA-1<sup>9</sup> and cryptographic key sizes none<sup>11</sup> that meet the following: FIPS 180-4<sup>12, 13</sup>.

FCS\_COP.1/ENC Cryptographic operation – Encryption / Decryption Triple DES

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/ ENC The TSF shall perform secure messaging (BAC) – encryption and decryption<sup>14</sup> in accordance with a specified cryptographic algorithm Triple-DES in CBC mode<sup>15</sup> and cryptographic key sizes 112 bit<sup>16</sup> that meet the following: FIPS 46-3 [13] and [8]; normative appendix 5, A5.3<sup>17</sup>.

FCS\_COP.1/MAC Cryptographic operation – Retail 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

<sup>8</sup> [assignment: *list of cryptographic operations*]

<sup>9</sup> [selection: *SHA-1 or other approved algorithms*]

<sup>10</sup> [assignment: *cryptographic algorithm*]

<sup>11</sup> [assignment: *cryptographic key sizes*]

<sup>12</sup> [selection: *FIPS 180-4 or other approved standards*]

<sup>13</sup> [assignment: *list of standards*]

<sup>14</sup> [assignment: *list of cryptographic operations*]

<sup>15</sup> [assignment: *cryptographic algorithm*]

<sup>16</sup> [assignment: *cryptographic key sizes*]

<sup>17</sup> [assignment: *list of standards*]

FCS\_COP.1.1/ MAC The TSF shall perform secure messaging – message authentication code <sup>18</sup> in accordance with a specified cryptographic algorithm Retail MAC <sup>19</sup> and cryptographic key sizes 112 bit <sup>20</sup> that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) <sup>21</sup>.

FCS\_COP.1/AUTH Cryptographic operation – Authentication

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes, or FDP\_ITC.2 Import of user data with security attributes, or FCS\_CKM.1 Cryptographic key generation] FCS\_CKM.4 Cryptographic key destruction

FCS\_COP.1.1/ AUTH The TSF shall perform symmetric authentication – encryption and decryption <sup>22</sup> in accordance with a specified cryptographic algorithm Triple-DES<sup>23</sup> and cryptographic key sizes 112 bit<sup>24</sup> that meet the following: FIPS 46-3 [13]<sup>25</sup>.

FCS\_COP.1/AA Cryptographic operation – Active Authentication

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes, or FDP\_ITC.2 Import of user data with security attributes, or FCS\_CKM.1 Cryptographic key generation] FCS\_CKM.4 Cryptographic key destruction

FCS\_COP.1.1/AA The TSF shall perform digital signature generation <sup>26</sup> in accordance with a specified cryptographic algorithm RSA<sup>27</sup> and cryptographic key sizes up to 2048 bit<sup>28</sup> that meet the following: [10], Annex D, and [17] Digital Signature scheme 1<sup>29</sup>.

Note that the SFR FCS\_COP.1/AA is only supported by the TOE in case the Active Authentication key pair is loaded during the personalization.

Note that the cryptographic operation FCS\_COP.1/AA accepts various key sizes up to 2048 bit. For security reason key size shorter than 2048 bit shall not be used.

### 6.1.2.2 Random Number Generation (FCS\_RND.1)

The TOE shall meet the requirement “Quality metric for random numbers (FCS\_RND.1)” as specified below (Common Criteria Part 2 extended).

FCS\_RND.1 Quality metric for random numbers

<sup>18</sup> [assignment: *list of cryptographic operations*]

<sup>19</sup> [assignment: *cryptographic algorithm*]

<sup>20</sup> [assignment: *cryptographic key sizes*]

<sup>21</sup> [assignment: *list of standards*]

<sup>22</sup> [assignment: *list of cryptographic operations*]

<sup>23</sup> [assignment: *cryptographic algorithm*]

<sup>24</sup> [assignment: *cryptographic key sizes*]

<sup>25</sup> [assignment: *list of standards*]

<sup>26</sup> [assignment: *list of cryptographic operations*]

<sup>27</sup> [assignment: *cryptographic algorithm*]

<sup>28</sup> [assignment: *cryptographic key sizes*]

<sup>29</sup> [assignment: *list of standards*]

Hierarchical to: No other components.

Dependencies: No dependencies.

- FCS\_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet the following quality metric:  
 (class DRG.4 of AIS20 [7]).  
 (DRG.4.6) The RNG generates output for which  $2^{48}$  strings of bit length 128 are mutually different with probability at least  $1 - 2^{-24}$ .  
 (DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A<sup>30</sup> (as defined in [7]).

### 6.1.3 Class FIA Identification and Authentication

The Table 4 provides an overview on the authentication mechanisms used.

**Table 4. Overview on authentication SFR**

Name	SFR for the TOE	Algorithms and key sizes according to [8], normative appendix 5, and [22]
Basic Access Control Authentication Mechanism	FIA_UAU.4 and FIA_UAU.6	Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	either Triple-DES with 112 bit keys or AES with 128 up to 256 bit keys (cf. FCS_COP.1/AUTH)
Active Authentication	FIA_API.1	RSA and cryptographic key sizes up to 2048 bit

Note that the cryptographic operation FCS\_COP.1/AA accepts various key sizes up to 2048 bit. For security reason key size shorter than 2048 bit shall not be used.

The TOE shall meet the requirement “Timing of identification (FIA\_UID.1)” as specified below (Common Criteria Part 2).

FIA\_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

- FIA\_UID.1.1 The TSF shall allow
  1. to read the Initialization Data in Phase 2 “Manufacturing”,
  2. to read the random identifier in Phase 3 “Personalization of the MRTD”,
  3. to read the random identifier in Phase 4 “Operational Use”<sup>31</sup> on behalf of the user to be performed before the user is

<sup>30</sup> [assignment: *additional test suites*]

<sup>31</sup> [assignment: *list of TSF-mediated actions*]

identified.

FIA\_UID.1.2

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

The TOE shall meet the requirement “Timing of authentication (FIA\_UAU.1)” as specified below (Common Criteria Part 2).

FIA\_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA\_UID.1 Timing of identification.

FIA\_UAU.1.1

The TSF shall allow

1. to read the Initialization Data in Phase 2 “Manufacturing”,
2. to read the random identifier in Phase 3 “Personalization of the MRTD”,
3. to read the random identifier in Phase 4 “Operational Use”<sup>32</sup>

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

FIA\_UAU.1.2

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

The TOE shall meet the requirements of “Single-use authentication mechanisms (FIA\_UAU.4)” as specified below (Common Criteria Part 2).

FIA\_UAU.4 Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA\_UAU.4.1

The TSF shall prevent reuse of authentication data related to

1. Basic Access Control Authentication Mechanism,
2. Authentication Mechanism based on Triple-DES<sup>33</sup>.

The TOE shall meet the requirement “Multiple authentication mechanisms (FIA\_UAU.5)” as specified below (Common Criteria Part 2).

FIA\_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA\_UAU.5.1

The TSF shall provide

1. Basic Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on Triple-DES<sup>34</sup>

to support user authentication.

<sup>32</sup> [assignment: *list of TSF-mediated actions*]

<sup>33</sup> [assignment: *identified authentication mechanism(s)*]

<sup>34</sup> [assignment: *list of multiple authentication mechanisms*]



FIA\_UAU.5.2 The TSF shall authenticate any user’s claimed identity according to the following rules:

1. the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s) the Symmetric Authentication Mechanism with the Personalization Agent Key,
2. the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys<sup>35</sup>.

The TOE shall meet the requirement “Re-authenticating (FIA\_UAU.6)” as specified below (Common Criteria Part 2).

FIA\_UAU.6 Re-authenticating – Re-authenticating of Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA\_UAU.6.1 The TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism<sup>36</sup>.

The TOE shall meet the requirement “Authentication failure handling (FIA\_AFL.1)” as specified below (Common Criteria Part 2).

Authentication failure handling (FIA\_AFL.1)

Hierarchical to: No other components.

Dependencies: FIA\_UAU.1 Timing of authentication

FIA\_AFL.1.1 The TSF shall detect when number in column 1 of Table 5<sup>37</sup> unsuccessful authentication attempts occur related to events in column 2 of Table 5<sup>38</sup>.

FIA\_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met<sup>39</sup>, the TSF shall return an action defined in column 3 of Table 5<sup>40</sup>.

**Table 5. Operations performed in FIA\_AFL.1**

<b>Column 1: FIA_AFL.1.1 assignment: positive number</b>	<b>Column 2: FIA_AFL.1.1 Assignment: list of authentication events</b>	<b>Column 3: FIA_AFL.1.2 assignment: list of actions</b>
10	Unsuccessful authentication attempt with Document Basic Access MAC Key (K <sub>MAC</sub> ) as Basic Inspection System for the first command of a session (cf.	After 10 unsuccessful authentication attempt a power-on reset is need to restart the device

<sup>35</sup> [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

<sup>36</sup> [assignment: *list of conditions under which re-authentication is required*]

<sup>37</sup> [assignment: *positive integer number*]

<sup>38</sup> [assignment: *list of authentication events*]

<sup>39</sup> [assignment: *met or surpassed*]

<sup>40</sup> [assignment: *list of actions*]

Column 1: FIA_AFL.1.1 assignment: positive number	Column 2: FIA_AFL.1.1 Assignment: list of authentication events	Column 3: FIA_AFL.1.2 assignment: list of actions
	FIA_UAU.5)	
1	Unsuccessful authentication attempt with Document Basic Access MAC Key (KMAC) for received command after the first command of a session with Basic Inspection System (cf. FIA_UAU.6)	Session with Document Basic Access Keys (KENC and KMAC) closed
14	Unsuccessful authentication attempt as Personalization Agent with Personalization Agent Authentication Key	Personalization Agent Authentication Key is blocked

The TOE shall meet the requirement “Authentication Proof of Identity (FIA\_API.1)” as specified below (Common Criteria Part 2 extended).

FIA_API.1	Authentication Proof of Identity
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide an <u>Active Authentication Protocol according to [8]</u> <sup>41</sup> to prove the identity of the <u>TOE</u> <sup>42</sup> to an external entity.

**Refinement: External entity is the Basic Inspection System.**

Note FIA\_API.1 may be disabled according to FMT\_SMF.1. The Active Authentication is only supported by the TOE in case the Active Authentication key pair is loaded during the personalization.

## 6.1.4 Class FDP User Data Protection

### 6.1.4.1 Subset access control for Basic Access Control

The TOE shall meet the requirement “Subset access control (FDP\_ACC.1)” as specified below (Common Criteria Part 2).

FDP\_ACC.1/BAC Subset access control – Basic Access control

Hierarchical to: No other components.

Dependencies: FDP\_ACF.1 Security attribute based access control

FDP_ACC.1.1/BAC	The TSF shall enforce the <u>Basic Access Control SFP</u> <sup>43</sup> on <u>terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD</u> <sup>44</sup> .
-----------------	--

Note that the logical MRTD in the protection profile BSI-CC-PP-0055 addresses all data groups. This TOE supports a subset of these data groups as detailed in section 2.4 and 3.1.

<sup>41</sup> [assignment: *authentication mechanism*]

<sup>42</sup> [selection: *TOE*, [assignment: *object, authorized user or role*]]

<sup>43</sup> [assignment: *access control SFP*]

<sup>44</sup> [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

#### 6.1.4.2 Security attribute based access control for Basic Access Control

The TOE shall meet the requirement “Security attribute based access control (FDP\_ACF.1)” as specified below (Common Criteria Part 2).

FDP\_ACF.1/BAC Basic Security attribute based access control – Basic Access Control

Hierarchical to: No other components.

Dependencies: FDP\_ACC.1 Subset access control

FMT\_MSA.3 Static attribute initialization

FDP_ACF.1.1/BAC	The TSF shall enforce the <u>Basic Access Control SFP</u> <sup>45</sup> to objects based on the following: <ol style="list-style-type: none"> <li>1. <u>Subjects:</u> <ol style="list-style-type: none"> <li>a. <u>Personalization Agent.</u></li> <li>b. <u>Basic Inspection System.</u></li> <li>c. <u>Terminal.</u></li> </ol> </li> <li>2. <u>Objects:</u> <ol style="list-style-type: none"> <li>a. <u>data EF.DG1 to EF.DG16 of the logical MRTD.</u></li> <li>b. <u>data in EF.COM.</u></li> <li>c. <u>data in EF.SOD.</u></li> </ol> </li> <li>3. <u>Security attributes</u> <ol style="list-style-type: none"> <li>a. <u>authentication status of terminals</u> <sup>46</sup>.</li> </ol> </li> </ol>
FDP_ACF.1.2/BAC	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: <ol style="list-style-type: none"> <li>1. <u>the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD.</u></li> <li>2. <u>the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD</u><sup>47</sup>.</li> </ol>
FDP_ACF.1.3/BAC	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none</u> <sup>48</sup> .
FDP_ACF.1.4/BAC	The TSF shall explicitly deny access of subjects to objects based on the <u>rule:</u> <ol style="list-style-type: none"> <li>1. <u>Any Terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.</u></li> <li>2. <u>Any Terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.</u></li> <li>3. <u>The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.</u> <sup>49</sup>.</li> </ol>

<sup>45</sup> [assignment: *access control SFP*]

<sup>46</sup> [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*]

<sup>47</sup> [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

<sup>48</sup> [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

<sup>49</sup> [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

Note that the logical MRTD in the protection profile BSI-CC-PP-0055 addresses all data groups. This TOE supports a subset of these data groups as detailed in section 2.4 and 3.1.

#### 6.1.4.3 Inter-TSF-Transfer

The TOE shall meet the requirement “Basic data exchange confidentiality (FDP\_UCT.1)” as specified below (Common Criteria Part 2).

FDP\_UCT.1 Basic data exchange confidentiality - MRTD

Hierarchical to: No other components.

Dependencies: [FTP\_ITC.1 Inter-TSF trusted channel, or  
FTP\_TRP.1 Trusted path]  
[FDP\_ACC.1 Subset access control, or  
FDP\_IFC.1 Subset information flow control]

FDP\_UCT.1.1 The TSF shall enforce the Basic Access Control SFP<sup>50</sup> to be able to transmit and receive<sup>51</sup> user data in a manner protected from unauthorized disclosure.

The TOE shall meet the requirement “Data exchange integrity (FDP\_UIT.1)” as specified below (Common Criteria Part 2).

FDP\_UIT.1 Data exchange integrity - MRTD

Hierarchical to: No other components.

Dependencies: [FDP\_ACC.1 Subset access control, or  
FDP\_IFC.1 Subset information flow control]  
[FTP\_ITC.1 Inter-TSF trusted channel, or  
FTP\_TRP.1 Trusted path]

FDP\_UIT.1.1 The TSF shall enforce the Basic Access Control SFP<sup>52</sup> to be able to transmit and receive<sup>53</sup> user data in a manner protected from modification, deletion, insertion and replay<sup>54</sup> errors.

FDP\_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay<sup>55</sup> has occurred.

#### 6.1.4.4 Subset access control Active Authentication

The TOE shall meet the requirement “Subset access control (FDP\_ACC.1)” as specified below (Common Criteria Part 2).

FDP\_ACC.1/AA Subset access control – Active Authentication

Hierarchical to: No other components.

Dependencies: FDP\_ACF.1 Security attribute based access control

<sup>50</sup> [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

<sup>51</sup> [selection: *transmit, receive*]

<sup>52</sup> [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

<sup>53</sup> [selection: *transmit, receive*]

<sup>54</sup> [selection: *modification, deletion, insertion, replay*]

<sup>55</sup> [selection: *modification, deletion, insertion, replay*]

FDP\_ACC.1.1/AA The TSF shall enforce the Active Authentication SFP<sup>56</sup> on

1. subjects
  - a. Personalization Agent,
  - b. Basic Inspection System,
  - c. Any Terminal.
2. objects and operations:
  - a. write and use Active Authentication Private Key,
  - b. write and export Active Authentication Public Key<sup>57</sup>.

### 6.1.4.5 Security attribute based access control Active Authentication

The TOE shall meet the requirement “Security attribute based access control (FDP\_ACF.1)” as specified below (Common Criteria Part 2).

FDP\_ACF.1/AA Basic Security attribute based access control – Active Authentication

Hierarchical to: No other components.

Dependencies: FDP\_ACC.1 Subset access control  
FMT\_MSA.3 Static attribute initialization

FDP\_ACF.1.1/AA The TSF shall enforce the Active Authentication SFP<sup>58</sup> to objects based on the following:

1. Subjects:
  - a. Personalization Agent,
  - b. Basic Inspection System,
  - c. Any Terminal.
2. Objects:
  - a. Active Authentication Public Keys (EF.DG15),
  - b. Active Authentication Private Keys,
3. Security attributes
  - a. authentication status of terminals<sup>59</sup>.

FDP\_ACF.1.2/AA The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. The successfully authenticated Personalization Agent is allowed to write the Active Authentication Private Key.
2. The successfully authenticated Personalization Agent is allowed to write the Active Authentication Public Key into EF.DG15.
3. The successfully authenticated Basic Inspection System is allowed to read the Active Authentication from EF.DG15.<sup>60</sup>

FDP\_ACF.1.3/AA The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

1. Any Terminal is allowed to use the Active Authentication Private

<sup>56</sup> [assignment: *access control SFP*]

<sup>57</sup> [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

<sup>58</sup> [assignment: *access control SFP*]

<sup>59</sup> [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*]

<sup>60</sup> [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

FDP\_ACF.1.4/AA Key to generate signatures<sup>61</sup>.  
 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1. No terminal is allowed to read the Active Authentication Private Key.
2. Any Terminal and Basic Inspection System are not allowed to write the Active Authentication Private Key.<sup>62</sup>.

## 6.1.5 Class FMT Security Management

The TOE shall meet the requirement “Specification of Management Functions (FMT\_SMF.1)” as specified below (Common Criteria Part 2).

FMT\_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No Dependencies

FMT\_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. Initialization.
2. Pre-personalization.
3. Personalization
4. **Enabling and disabling of Active Authentication in Personalization Phase by storing the key pair to the intended memory areas**<sup>63</sup>.

The TOE shall meet the requirement “Security roles (FMT\_SMR.1)” as specified below (Common Criteria Part 2).

FMT\_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA\_UID.1 Timing of identification.

FMT\_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer.
2. Personalization Agent.
3. Basic Inspection System<sup>64</sup>.

FMT\_SMR.1.2 The TSF shall be able to associate users with roles.

The TOE shall meet the requirement “Limited capabilities (FMT\_LIM.1)” as specified below (Common Criteria Part 2 extended).

FMT\_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT\_LIM.2 Limited availability.

<sup>61</sup> [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

<sup>62</sup> [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

<sup>63</sup> [assignment: list of management functions to be provided by the TSF]

<sup>64</sup> [assignment: the authorised identified roles]

FMT\_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT\_LIM.2)” the following policy is enforced:

Deploying Test Features after TOE Delivery does not allow

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

The TOE shall meet the requirement “Limited availability (FMT\_LIM.2)” as specified below (Common Criteria Part 2 extended).

FMT\_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT\_LIM.1 Limited capabilities.

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

Deploying Test Features after TOE Delivery does not allow

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

The TOE shall meet the requirement “Management of TSF data (FMT\_MTD.1)” as specified below (Common Criteria Part 2). The iterations address different management functions and different TSF data.

FMT\_MTD.1/INI\_ENA Management of TSF data – Writing of Initialization Data and Pre-personalization Data

Hierarchical to: No other components.

Dependencies: FMT\_SMF.1 Specification of management functions  
FMT\_SMR.1 Security roles

FMT\_MTD.1.1/INI\_ENA The TSF shall restrict the ability to write<sup>65</sup> the Initialization Data and Pre-personalization Data<sup>66</sup> to the Manufacturer<sup>67</sup>.

FMT\_MTD.1/INI\_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data

Hierarchical to: No other components.

Dependencies: FMT\_SMF.1 Specification of management functions  
FMT\_SMR.1 Security roles

FMT\_MTD.1.1/INI\_DIS The TSF shall restrict the ability to disable read access for users to<sup>68</sup> the Initialization Data<sup>69</sup> to the Personalization Agent<sup>70</sup>.

<sup>65</sup> [selection: *change\_default, query, modify, delete, clear*, [assignment: *other operations*]]

<sup>66</sup> [assignment: *list of TSF data*]

<sup>67</sup> [assignment: *the authorised identified roles*]

FMT\_MTD.1/KEY\_WRITE Management of TSF data – Key Write

Hierarchical to: No other components.

Dependencies: FMT\_SMF.1 Specification of management functions  
 FMT\_SMR.1 Security roles

FMT\_MTD.1.1/  
 KEY\_WRITE The TSF shall restrict the ability to write<sup>71</sup> the Document Basic Access Keys and the Active Authentication Key<sup>72</sup> to the Personalization Agent<sup>73</sup>.

FMT\_MTD.1/KEY\_READ Management of TSF data – Key Read

Hierarchical to: No other components.

Dependencies: FMT\_SMF.1 Specification of management functions  
 FMT\_SMR.1 Security roles

FMT\_MTD.1.1/  
 KEY\_READ The TSF shall restrict the ability to read<sup>74</sup> the Document Basic Access Keys, the Active Authentication Private Key and Personalization Agent Keys<sup>75</sup> to none<sup>76</sup>.

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

## 6.1.6 Class FPT Protection of the Security Functions

The TOE shall meet the requirement “TOE Emanation (FPT\_EMS.1)” as specified below (Common Criteria Part 2 extended).

FPT\_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT\_EMS.1.1 The TOE shall not emit electromagnetic and current emissions<sup>77</sup> in excess of non useful information<sup>78</sup> enabling access to Personalization Agent Key(s), Document Basic Access Keys and Active Authenticate Private Key if implemented (cf. FMT\_SMF.1)<sup>79</sup> and EF.COM, EF.SOD, EF.DG1, EF.DG2, and EF.DG6 to EF.DG14 and EF.DG16<sup>80</sup>.

<sup>68</sup> [selection: *change\_default, query, modify, delete, clear*, [assignment: *other operations*]]

<sup>69</sup> [assignment: *list of TSF data*]

<sup>70</sup> [assignment: *the authorised identified roles*]

<sup>71</sup> [selection: *change\_default, query, modify, delete, clear*, [assignment: *other operations*]]

<sup>72</sup> [assignment: *list of TSF data*]

<sup>73</sup> [assignment: *the authorised identified roles*]

<sup>74</sup> [selection: *change\_default, query, modify, delete, clear*, [assignment: *other operations*]]

<sup>75</sup> [assignment: *list of TSF data*]

<sup>76</sup> [assignment: *the authorised identified roles*]

<sup>77</sup> [assignment: *types of emissions*]

<sup>78</sup> [assignment: *specified limits*]

<sup>79</sup> [assignment: *list of types of TSF data*]

<sup>80</sup> [assignment: *list of types of user data*]



FPT\_EMS.1.2 The TSF shall ensure any unauthorized users<sup>81</sup> are unable to use the following interface smart card circuit contacts<sup>82</sup> to gain access to Personalization Agent Key(s), Document Basic Access Keys and Active Authenticate Private Key if implemented (cf. FMT\_SMF.1)<sup>83</sup> and EF.COM, EF.SOD, EF.DG1, EF.DG2, and EF.DG6 to EF.DG14 and EF.DG16<sup>84</sup>.

Note that the logical MRTD in the protection profile BSI-CC-PP-0055 addresses all data groups. This TOE supports a subset of these data groups as detailed in section 2.4 and 3.1.

The following security functional requirements address the protection against forced illicit information leakage including physical manipulation.

The TOE shall meet the requirement “Failure with preservation of secure state (FPT\_FLS.1)” as specified below (Common Criteria Part 2).

FPT\_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No Dependencies.

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

1. Exposure to out-of-range operating conditions where therefore a malfunction could occur.
2. failure detected by TSF according to FPT\_TST.1<sup>85</sup>.

The TOE shall meet the requirement “TSF testing (FPT\_TST.1)” as specified below (Common Criteria Part 2).

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 start-up<sup>86</sup> to demonstrate the correct operation of the TSF<sup>87</sup>.

FPT\_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data<sup>88</sup>.

FPT\_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

The TOE shall meet the requirement “Resistance to physical attack (FPT\_PHP.3)” as specified below (Common Criteria Part 2).

FPT\_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

<sup>81</sup> [assignment: *type of users*]

<sup>82</sup> [assignment: *type of connection*]

<sup>83</sup> [assignment: *list of types of TSF data*]

<sup>84</sup> [assignment: *list of types of user data*]

<sup>85</sup> [assignment: *list of types of failures in the TSF*]

<sup>86</sup> [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]*]

<sup>87</sup> [selection: [assignment: *parts of TSF*], *the TSF*]

<sup>88</sup> [selection: [assignment: *parts of TSF*], *TSF data*]

Dependencies: No dependencies.

FPT\_PHP.3.1 The TSF shall resist physical manipulation and physical probing <sup>89</sup> to the TSF <sup>90</sup> by responding automatically such that the SFRs are always enforced.

## 6.2 Security Assurance Requirements for the TOE

For the evaluation of the TOE and its development and operating environment the assurance requirements are taken from the

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ALC\_DVS.2 and ATE\_DPT.2.

## 6.3 Security Requirements Rationale

### 6.3.1 Security Functional Requirements Rationale

The following table provides an overview for security functional requirements coverage.

**Table 6. Coverage of Security Objective for the TOE by SFR**

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func	OT.Active_Auth_Proof
FAU_SAS.1				x					
FCS_CKM.1	x	x	x						
FCS_CKM.4	x		x						
FCS_COP.1/SHA	x	x	x						
FCS_COP.1/ENC	x	x	x						
FCS_COP.1/AUTH	x	x							
FCS_COP.1/MAC	x	x	x						
FCS_COP.1/AA									x
FCS_RND.1	x	x	x						
FIA_UID.1			x	x					
FIA_AFL.1			x	x					
FIA_UAU.1			x	x					
FIA_UAU.4	x	x	x						
FIA_UAU.5	x	x	x						
FIA_UAU.6	x	x	x						

<sup>89</sup> [assignment: *physical tampering scenarios*]

<sup>90</sup> [assignment: *list of TSF devices/elements*]

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func	OT.Active_Auth_Proof
FIA_API.1									X
FDP_ACC.1/BAC	X	X	X						X
FDP_ACF.1/BAC	X	X	X						X
FDP_ACC.1/AA									X
FDP_ACF.1/AA									X
FDP_UCT.1	X	X	X						
FDP_UIT.1	X	X	X						
FMT_SMF.1	X	X	X						X
FMT_SMR.1	X	X	X						
FMT_LIM.1								X	
FMT_LIM.2								X	
FMT_MTD.1/INI_ENA				X					
FMT_MTD.1/INI_DIS				X					
FMT_MTD.1/KEY_WRITE	X	X	X						X
FMT_MTD.1/KEY_READ	X	X	X						X
FPT_EMS.1	X				X				
FPT_TST.1					X		X		
FPT_FLS.1	X				X		X		
FPT_PHP.3	X				X	X			

The detailed justification for the security requirements rationale and the security objectives defined in the Protection Profile [19] is already provided in this Protection Profile. The following table includes an overview of the modified and added security functional requirements:

**Table 7. Overview of modified and added Security Functional Requirements**

SFR	Rationale
FCS_COP.1/AA	The SFR defines an additional iteration of FCS_COP.1 for the asymmetric chip authentication. It is an additional functionality compared to [19].
FIA_API.1	The SFR defines an authentication method to authenticate the TOE based on FCS_COP.1/AA. It is an additional functionality compared to [19]. This authentication is only available if the Active Authentication key pair is written in the TOE. The Active Authentication is an optional authentication requested by the Basic Inspection System to authenticate the chip.
FDP_ACC.1/AA	The SFR is an iteration of FDP_ACC.1 with the additional access control for the Active Authentication key pair. It is an additional functionality compared to [19].

SFR	Rationale
FDP_ACF.1/AA	The SFR is an iteration of FDP_ACF.1 with the additional access control for the Active Authentication key pair considering the private key component and the public key component. It is an additional functionality compared to [19].
FMT_SMF.1	The assignment of the "list of management functions to be provided by the TSF" was supplemented with enabling and disabling of the Active Authentication. The management is limited to the additional functionality introduced by Active Authentication.
FMT_MTD.1/KEY_WRITE	The assignment of the "list of TSF data" was supplemented with the Active Authentication Key. The Active Authentication Key needs to be written and managed by the Personalization Agent in the same way as the Document Basic Access Keys. There is was possible to supplement this assignment.
FMT_MTD.1/KEY_READ	The assignment of the "list of TSF data" was supplemented with with the Active Authentication Private Key. Read access and management of the Personalization Agent shall be restricted in the same way as the Document Basic Access Keys. There is was possible to supplement this assignment.

The change of security functional requirements is limited to the extension of assignments. The extensions are based on the additional Active Authentication that can be enabled and disabled during the personalization. In addition new security functional requirements are added either using an iteration if they were already used or by adding new Security Functional Requirements. The security functional requirements added in this Security Target Lite EP-COS V3.0 do not impact the set of definitions already included in the Protection Profile. Therefore the rationale included in the Protection Profile remains valid and is not reproduced here. In the following the rationale for the extensions is provided.

The security objective **OT.Active\_Auth\_Proof** "Proof of MRTD's chip authenticity by means of Active Authentication" is covered by (i) FMT\_MTD.1/KEY\_WRITE the storage of Active Authentication Key Pairs, (ii) FCS\_COP.1/AA for digital signature generation used for Active Authentication, (iii) FIA\_API.1 requiring support of TOE authentication to the Basic Inspection System, (iv) FDP\_ACC.1/BAC and FDP\_ACF.1/BAC controlling write and read access to EF.DG15 containing the Active Authentication Public Key if Active Authentication is enabled according to FMT\_SMF.1, (v) FDP\_ACC.1/AA and FDP\_ACF.1/AA controlling access to, write and use the Active Authentication Private Key and export and use Active Authentication Public Key, and (vi) FMT\_SMF.1 addressing enabling and disabling Active Authentication in the Personalization Phase. FMT\_MTD.1/KEY\_READ prevents read access to the Active Authentication Private Key and ensure together with the SFR FPT\_EMSEC.1, FPT\_FLS.1 and FPT\_PHP.3 the confidentiality of the Active Authentication Private Key.

Note: Although any terminal can initiate the generation of a signature by the TOE, a verification of the signature is only possible after reading DG15 and EF.SOD that can only be read by a Basic Inspection System after successful BAC authentication.

### 6.3.2 Dependency Rationale

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-dissolved dependencies are appropriately explained.

The Table 8 shows the dependencies between the SFR of the TOE.

**Table 8. Dependencies between the SFR for the TOE**

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction,	Fulfilled by FCS_COP.1/ENC and FCS_COP.1/MAC,  Fulfilled by FCS_CKM.4
FCS_CKM.4	[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,
FCS_COP.1/SHA	[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	justification 1 for non-satisfied dependencies,  Fulfilled by FCS_CKM.4
FCS_COP.1/ENC	[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	Fulfilled by FCS_CKM.1,  Fulfilled by FCS_CKM.4
FCS_COP.1/AUTH	[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	justification 2 for non-satisfied dependencies  justification 2 for non-satisfied dependencies
FCS_COP.1/MAC	[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	Fulfilled by FCS_CKM.1,  Fulfilled by FCS_CKM.4

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/AA	[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	justification 7 for non-satisfied dependencies  justification 5 for non-satisfied dependencies
FCS_RND.1	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FIA_API.1	No dependencies	n.a.
FDP_ACC.1/BAC	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/BAC
FDP_ACF.1/BAC	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/BAC, justification 3 for non-satisfied dependencies
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	justification 4 for non-satisfied dependencies  Fulfilled by FDP_ACC.1/BAC
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	justification 4 for non-satisfied dependencies  Fulfilled by FDP_ACC.1/BAC
FDP_ACC.1/AA	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/AA
FDP_ACF.1/AA	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/AA, justification 6 for non-satisfied dependencies
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1

SFR	Dependencies	Support of the Dependencies
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FPT_EMS.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

Justification for non-satisfied dependencies between the SFR for TOE:

No. 1: 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.

No. 2: The SFR FCS\_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT\_MTD.1/INI\_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE lifecycle by the means of FCS\_CKM.1 or FDP\_ITC. Since the key is permanently stored within the TOE there is no need for FCS\_CKM.4, too.

No. 3: The access control TSF according to FDP\_ACF.1/BAC uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT\_MSA.1 and FMT\_MSA.3) is necessary here.

No. 4: The SFR FDP\_UCT.1 and FDP\_UIT.1 require the use secure messaging between the MRTD and the BIS. There is no need for SFR FTP\_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP\_TRP.1 is not applicable here.

No. 5: The Active Authentication Key Pair will not be destroyed if stored in the TOE.

No. 6: The access control TSF according to FDP\_ACF.1/AA uses security attribute authentication state of the terminal which gained by authentication. No management of these security attribute (i.e. SFR FMT\_MSA.1 and FMT\_MSA.3) is necessary here.

No. 7: The dependency to 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 is not fulfilled because the TOE restricts ability to load the Active Authentication key to the personalization phase. Only in case the key is loaded during personalization phase, the Active Authentication is enabled. The personalization is performed in the trusted environment of the Personalization Agent. Therefore the protection of the key pair is under control of the Personalization Agent.

### 6.3.3 Security Assurance Requirements Rationale

EAL4 augmented by ALC\_DVS.2 is required by the protection profile BSI-CC-PP-0055 [\[19\]](#) which is claimed in this Security Target Lite EP-COS V3.0. ATE\_DPT.2 was required by the version of Common Criteria referenced in the Protection Profile [\[19\]](#).

### 6.3.4 Security Requirements – Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form a mutually supportive and internally consistent whole.

The analysis of the TOE's security requirements with regard to their mutual support and internal consistency demonstrates:

The "Dependency Rationale" in section [6.3.2](#) for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the "Security Assurance Requirements Rationale" in section [6.3.3](#) shows that the assurance requirements are internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections [6.3.2 "Dependency Rationale"](#) and [6.3.3 "Security Assurance Requirements Rationale"](#). Furthermore, as also discussed in section [6.3.3](#), the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.



## 7. TOE Summary Specification

This TOE summary specification describes how the TOE meets each SFR. The TSF is provided by the circuitry of the MRTD's chip P60D081PVB and by the embedded software of the MRTD's chip, the Crypto Library V3.1.2 on P60D081PVB and the operating system as enabled by the object system BAC with AA V2.0.

FMT\_SMR.1 and FMT\_SMF.1 define the required roles and security management functions of the TOE. FMT\_LIM.1 Limited capabilities and FMT\_LIM.2 Limited availability protect user and TSF data over the life cycle of the TOE.

### Personalization of initialized TOE

The MRTD chip is initialized chip before the delivery by the IC manufacturer with a Personalization Agent authentication key stored on the TOE. The IC manufacturer writes the Initialization Data and the audit records of the IC during the Phase 2 "Manufacturing". In addition a data set provided by the MRTD developer including the Personalization Agent authentication key is written by the IC manufacturer in non-volatile memory of the TOE. The Initialization Data, Pre-personalization Data and audit records can be written only in Phase 2 Manufacturing of the TOE, cf. FAU\_SAS.1 and FMT\_MTD.1/INI\_ENA. After delivery of the chip by the IC Manufacturer the personalization agent can unlock the chip by authentication with the Personalization Agent authentication key. After personalization the Initialization Data and Pre-personalization Data cannot be read as defined by FMT\_MTD.1/INI\_DIS. The personalization agent can use the Personalization Agent authentication key but cannot read this key according to FMT\_MTD.1/KEY\_READ. As specified by FIA\_UID.1 and FIA\_UAU.1 the mutual authentication must be performed to unlock the device and allow further commands.

The Personalization Authentication Key is used for authentication of the Personalization Agent according to FIA\_UAU.4 and FIA\_UAU.5. The users in role Personalization Agent identify themselves by means of selecting the authentication key and running mutual authentication FCS\_COP.1/AUTH with a challenge-response protocol based on the symmetric key. After the authentication of the Personalization Agent, this role can perform the personalization. At the end of the personalization in Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The authentication attempt of the Personalization Agent is blocked according to FIA\_AFL.1 after fourteen unsuccessful authentication attempts.

The Active Authentication can be disabled at the state of TOE personalization as specified by FMT\_SMF.1. If no Active Authentication Key is stored on the TOE the internal authenticate command is not supported. The Personalization Agent enables Active Authentication by writing the Active Authentication Key Pair according to FMT\_MTD.1/KEY\_WRITE and under access control according to FDP\_ACC.1/AA and FDP\_ACF.1/AA. The public key component is stored in DG15 and the private key component is stored in an internal key file that is read protected according to FMT\_MTD.1/KEY\_READ.

Personalization of the TOE including writing the Basic Access Control keys is controlled by the access control policy defined by FDP\_ACC.1/BAC and FDP\_ACF.1/BAC. The control of the Active Authentication key during the personalization is defined by the access control policy FDP\_ACC.1/AA and FDP\_ACF.1/AA.

### Basic Access Control

The processes before successful identification and authentication are limited according to the control of FIA\_UID.1 and FIA\_UAU.1, i.e. the operating system and the object system require authentication. Note that the generation of a signature based on the internal authenticate command is not considered as TSF-mediated action because the signature can only be verified using the public key stored in DG15 and the associated signature to verify the authenticity of the public key stored in EF:SOD. DG15 and EF.SOD can only be read after successful BAC authentication and established secure messaging.

The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key for mutual authentication with the Basic Inspection System according to FIA\_UAU.4 and FIA\_UAU.5 and using FCS\_CKM.1 with support of FCS\_COP.1/SHA to generate the session keys for FCS\_COP.1/ENC and FCS\_COP.1/MAC. The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [8]. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip authenticates to the terminal in the second step. In this second step the MRTD's chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. The required random numbers of the challenge-response and the session keys derivation are generated by a deterministic random number generator according to FCS\_RND.1. The TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol based on FIA\_AFL.1. Further FIA\_AFL.1 prevents guessing by time delays after unsuccessful authentication attempts of the Basic Inspection System. Authentication attempts are delayed by the TOE requiring a power on reset after 10 unsuccessful authentication attempts. The secure messaging is required for all following command APDUs received by the TOE according FIA\_UAU.6 using cryptographic operation implemented as required by FCS\_COP.1/MAC and FCS\_COP.1/ENC except for the Active Authentication based on FCS\_COP.1/AA. The TOE checks by secure messaging in MAC\_ENC mode each received command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS\_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code and the session is closed after unsuccessful verification of MAC according to FIA\_AFL.1. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user based on FIA\_UAU.6. Based on the mutual authentication and the session key generation according FCS\_CKM.1 with support of FCS\_COP.1/SHA the two session keys for FCS\_COP.1/MAC. and FCS\_COP.1/ENC are derived. The secure messaging also implements the integrity protection by means of FDP\_UIT.1 and confidentiality according FDP\_UCT.1. FCS\_CKM.4 is used to destruct session key of the secure channel between TOE and Basic Inspection System after the session is terminated or an error occurred. Access control to keys and data based on successful authentication between Basic Inspection System and TOE is defined by FDP\_ACC.1/BAC and FDP\_ACF.1/BAC. Active Authentication has no impact on the access control since it is optional.

### Active Authentication

The Active Authentication according to FIA\_API.1 is performed by a challenge-response using the cryptographic mechanism FCS\_COP.1/AA if the Active Authentication Key is written to the TOE during personalization according to FMT\_SMF.1. The Active Authentication is optional even if it is enabled and has no impact on the access control to

data defined in FDP\_ACC.1/BAC and FDP\_ACF.1/BAC. The usage, access control and export conditions for the public key component of the Active Authentication key pair is defined by FDP\_ACC.1/AA and FDP\_ACF.1/AA. FDP\_ACC.1/AA and FDP\_ACF.1/AA also define the usage of the private key component. In addition read access to the private key component is prevented according to FMT\_MTD.1/KEY\_READ.

### TSF protection

The security IC provide FPT\_TST.1, FPT\_PHP.3 and FPT\_FLS.1 as described in ST for the chip P60D081PVB and by the embedded software of the MRTD’s chip, the Crypto Library V3.1.2 on P60D081PVB. FPT\_EMS.1 protects the Personalization Agent Authentication Key and Active Authentication Key if Active Authentication is enabled and other secrets like session keys of the secure messaging channel between TOE and Basic Inspection System.

The operating system provides FPT\_EMS.1 for the user transmitted through the secure messaging channel as enabled by the object system BAC with AA V2.0

The self-test for the verification of the integrity of stored TSF executable code required by FPT\_TST.1.3 is executed during initial start-up by the “authorized user” Manufacturer in the Phase 2 Manufacturing. Other self-tests run automatically to detect failure and to preserve of secure state according to FPT\_FLS.1 in the Phase 4 “Operational Use”, e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks.

## 7.1 Compatibility

This composite Security Target Lite EP-COS V3.0 is based on an underlying hardware platform. The security functionality of the hardware platform is described in [20]. Further on the composite product uses the crypto library provided for the hardware platform. The security functionality of the crypto library is described in [21].

The following table provides a mapping between the security services and security functionality provided by the hardware platform and the cryptographic library with the security functionality provided by the composite TOE.

According to the Security Target of the crypto library [21] the crypto library used the underlying coprocessors to perform cryptographic operations. Since this mapping is already provided in [21] it is not reproduced here.

**Table 9. Mapping of security functionality provided by the composite product**

	FMT_LIM.1 (Chip)	FMT_LIM.2 (Chip)	FPT_FLS.1 (Chip)	FPT_PHP.3 (Chip)	FAU_SAS.1 (Chip)	FCS_RNG.1[HYB-DET] (CL)	FCS_COP.1[SW_DES] (CL)	FCS_COP.1[SHA] (CL)	FCS_COP.1[RSA] (CL)	FDP_RIP.1(CL)	FCS_CKM.4 (CL)	FDP_SOP.1[Compare] (CL)	FDP_SOP.1[Copy] (CL)
FAU_SAS.1					X								
FCS_CKM.1							X						
FCS_CKM.4													

	FMT_LIM.1 (Chip)	FMT_LIM.2 (Chip)	FPT_FLS.1 (Chip)	FPT_PHP.3 (Chip)	FAU_SAS.1 (Chip)	FCS_RNG.1[HYB-DET] (CL)	FCS_COP.1[SW_DES] (CL)	FCS_COP.1[SHA] (CL)	FCS_COP.1[RSA] (CL)	FDP_RIP.1(CL)	FCS_CKM.4 (CL)	FDP_SOP.1[Compare] (CL)	FDP_SOP.1[Copy] (CL)
FCS_COP.1/SHA								X					
FCS_COP.1/ENC							X						
FCS_COP.1/AUTH							X						
FCS_COP.1/MAC							X						
FCS_COP.1/AA									X				
FCS_RND.1						X							
FMT_LIM.1	X												
FMT_LIM.2		X											
FPT_FLS.1			X										
FPT_PHP.3				X									

The remaining security functional requirements of the composite TOE rely on the security functionality provided by the underlying hardware platform but a direct mapping is not possible for these security functional requirements. No conflicting security functional requirements between the hardware platform including crypto library and the composite TOE were identified that may require contrary functionality.

The detailed description is removed in this Security Target Lite.

The following table provides an overview of the assumptions of the underlying hardware platform and crypto library and identifies the significant assumptions for the composite product.

Assumption	Assignment	Significance
A.Process-Sec-IC	hardware platform	The Security IC Embedded Software addresses these assumptions and implements appropriate measures to protect the life cycle phases within the scope of the Security Target.
A.Resp-Appl	hardware platform	The Security IC Embedded Software addresses these assumptions and implements appropriate measures to protect security relevant user data.
A.Check-Init-Plain	hardware platform	Initialization data is generated by the MRDT developer to support identification, traceability and authentication during the Personalization.

Note that only assumptions of the hardware configuration "P VB" are included in the list since this is the target hardware configuration.

## 8. Glossary and Acronyms

The same definition of terms is used as in the glossary of [\[19\]](#). Therefore the glossary is not reproduced here.

**Table 10. Acronyms**

<b>Acronym</b>	<b>Term</b>
<i>AA</i>	Active Authentication
<i>BIS</i>	Basic Inspection System
<i>CC</i>	Common Criteria
<i>EF</i>	Elementary File
<i>GIS</i>	General Inspection System
<i>ICCSN</i>	Integrated Circuit Card Serial Number.
<i>MF</i>	Master File
<i>n.a.</i>	Not applicable
<i>OSP</i>	Organizational security policy
<i>PT</i>	Personalization Terminal
<i>SAR</i>	Security assurance requirements
<i>SFR</i>	Security functional requirement
<i>TOE</i>	Target of Evaluation
<i>TSF</i>	TOE security functions

## 9. Literature

---

### Common Criteria

- [1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
- [2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
- [3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012
- [4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
- [5] Anwendungshinweise und Interpretationen zum Schema, AIS32: Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema, Version 1, 02.07.2001, Bundesamt für Sicherheit in der Informationstechnik
- [6] Supporting Document Guidance Smartcard Evaluation February 2010, Version 2.0, CCDB-2010-03-001
- [7] AIS20/31: A proposal for: Functionality classes for random number generators, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.0, September 18th, 2011

### ICAO

- [8] ICAO Doc 9303, Machine Readable Travel Documents, Part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization
- [9] INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL) DIVISION, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)
- [10] ICAO Technical Report—Version 1.1—2004-10-01: Machine Readable Travel Documents: PKI for Machine Readable Travel Documents offering ICC Read-only Access
- [11] ICAO Doc 9303, Machine Readable Travel Documents, Part 3 - Machine Readable Official Travel Documents Volume 2: Specifications for electronically enabled official travel documents with biometric identification capabilities, 3rd Edition, 2008

### Cryptography

- [12] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999
- [13] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

- [14] Federal Information Processing Standards Publication 180-4 SECURE HASH STANDARD, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2015 August
- [15] Federal Information Processing Standards Publication 186-4 DIGITAL SIGNATURE STANDARD (DSS), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2013 July
- [16] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001
- [17] ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorization based mechanisms, 2002

#### Protection Profiles

- [18] Smartcard IC Platform Security Target with Augmentation package, Version 1.0, July 2014; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014
- [19] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application“, Basic Access Control, BSI-CC-PP-0055, Version 1.10, 25<sup>th</sup> March 2009

#### Security Targets

- [20] Security Target NXP Secure Smart Card Controller P6021y VB, Rev. 0.93, 25 January 2016 under reference BSI-DSZ-CC-0955
- [21] Security Target Crypto Library V3.1.x on P6021y VB, Rev. 1.4, 18 March 2016, under reference NSCIB-CC-15-66030

#### Other

- [22] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- [23] ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, 2004

## 10. Legal information

### 10.1 Definitions

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

### 10.2 Disclaimers

**Limited warranty and liability** — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the *Terms and conditions of commercial sale* of NXP Semiconductors.

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

**Suitability for use** — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors 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.

**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.

**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.

**Evaluation products** — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out of the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US\$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

### 10.3 Licenses

#### ICs with DPA Countermeasures functionality



NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

### 10.4 Patents

Notice is herewith given that the subject device uses one or more of the following patents and that each of these patents may have corresponding patents in other jurisdictions.

<Patent ID> — owned by <Company name>

### 10.5 Trademarks

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

<Name> — is a trademark of NXP Semiconductors N.V.



## 11. List of figures

---

Fig 1. FIA\_API.1 Authentication Proof of Identity..... 18

## 12. List of tables

---

Table 1.	Security Objective Rationale .....	15
Table 2.	Extended Components Definition.....	17
Table 3.	Definition of security attributes .....	19
Table 4.	Overview on authentication SFR.....	23
Table 5.	Operations performed in FIA_AFL.1 .....	25
Table 6.	Coverage of Security Objective for the TOE by SFR.....	34
Table 7.	Overview of modified and added Security Functional Requirements .....	35
Table 8.	Dependencies between the SFR for the TOE ..	37
Table 9.	Mapping of security functionality provided by the composite product.....	43
Table 10.	Acronyms .....	45

13. Contents

<b>1. ST Introduction</b> .....	<b>3</b>	6.3.3	Security Assurance Requirements Rationale ...	40
1.1 ST Reference .....	3	6.3.4	Security Requirements – Internal Consistency.	40
1.2 TOE Overview .....	3	<b>7. TOE Summary Specification</b> .....	<b>41</b>	
1.3 TOE Definition.....	3	7.1	Compatibility .....	43
<b>2. Conformance Claims</b> .....	<b>7</b>	<b>8. Glossary and Acronyms</b> .....	<b>45</b>	
2.1 CC Conformance Claim .....	7	<b>9. Literature</b> .....	<b>46</b>	
2.2 PP Claim .....	7	<b>10. Legal information</b> .....	<b>48</b>	
2.3 Package Claim .....	7	10.1	Definitions.....	48
2.4 Conformance Rationale .....	7	10.2	Disclaimers.....	48
<b>3. Security Problem Definition</b> .....	<b>10</b>	10.3	Licenses .....	48
3.1 Introduction .....	10	10.4	Patents .....	48
3.2 Assumptions.....	10	10.5	Trademarks .....	48
3.3 Threats.....	11	<b>11. List of figures</b> .....	<b>49</b>	
3.4 Organizational Security Policies.....	12	<b>12. List of tables</b> .....	<b>50</b>	
<b>4. Security Objectives</b> .....	<b>13</b>	<b>13. Contents</b> .....	<b>51</b>	
4.1 Security Objectives for the TOE .....	13			
4.2 Security Objectives for the Operational Environment .....	13			
4.3 Security Objective Rationale .....	14			
<b>5. Extended Components Definition</b> .....	<b>17</b>			
5.1 Definition of the Family FIA_API .....	17			
<b>6. Security Requirements</b> .....	<b>19</b>			
6.1 Security Functional Requirements for the TOE	20			
6.1.1 Class FAU Security Audit.....	20			
6.1.2 Class Cryptographic Support (FCS).....	20			
6.1.2.1 Cryptographic operation (FCS_COP.1).....	21			
6.1.2.2 Random Number Generation (FCS_RND.1)....	22			
6.1.3 Class FIA Identification and Authentication .....	23			
6.1.4 Class FDP User Data Protection.....	26			
6.1.4.1 Subset access control for Basic Access Control .....	26			
6.1.4.2 Security attribute based access control for Basic Access Control .....	27			
6.1.4.3 Inter-TSF-Transfer .....	28			
6.1.4.4 Subset access control Active Authentication....	28			
6.1.4.5 Security attribute based access control Active Authentication .....	29			
6.1.5 Class FMT Security Management .....	30			
6.1.6 Class FPT Protection of the Security Functions .....	32			
6.2 Security Assurance Requirements for the TOE	34			
6.3 Security Requirements Rationale.....	34			
6.3.1 Security Functional Requirements Rationale ...	34			
6.3.2 Dependency Rationale .....	36			

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