Security Target Lite EP-COS V3.0 Plain NSCIB-CC-127667

NXP Semiconductors Germany GmbH, Business Unit Security and Connectivity

Rev. 2.5 — 07 February 2022
408325

Document information

Info	Content
Keywords	ASE, EP-COS, Common Criteria, EAL4 augmented, Security Target Lite
Abstract	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
1.7	20170227	Security Target Lite derived from the complete Security Target version 1.7
2.5	20220207	Security Target Lite derived from the complete Security Target version 2.5

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 Plain
Document version:	Rev. 2.5
Date of document:	07 February 2022
TOE reference:	EP-COS V3.0 Plain Version EPCOSV30e
Certification ID:	NSCIB-CC-127667
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 Plain 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].

1.3 TOE Definition

TOE Description

The Target of Evaluation (TOE) EP-COS V3.0 Plain 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].

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), Version EPCOSV30e,
3. the MRTD application BAC (Version 1.0) and
4. the associated guidance documentation Personalization Guidance (AGD_PRE) EP-COS V3.0 Plain, Version 0.99 and Operational User Guidance (AGD_OPE) EP-COS V3.0 Plain, Version 0.98.

Part-1i.e. the circuitry of the MRTD's chip with crypto library along with Part-2 i.e. operating system is delivered by secure courier in module format to MRTD manufacturer for production of booklets.

Part-4 i.e. PGP encrypted AGD_PRE & AGD_OPE are emailed in pdf format via Field Application Engineer of NXP.

There is no separate deliverable for Part-3 i.e. the MRTD application BAC. It is created during personalization by personalization agent using knowledge (APDU commands) provided in AGD_PRE & AGD_OPE documents.

The circuitry of the MRTD's chip P60D081PVB is certified under certificate identification BSI-DSZ-CC-1072-V4-2021 and the Crypto Library V3.1.2 on P60D081PVB is certified under certificate identification NSCIB-CC-66030-CR5.

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.

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.

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

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 Plain claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 , [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017, [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017, [3]

as follows

- Part 2 extended,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017, [4]

has to be taken into account.

2.2 PP Claim

This Security Target Lite EP-COS V3.0 Plain 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 Plain 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 Plain 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. The data groups DG3 and DG4 are only supported if the MRTD supports extended access control. DG5 to DG10 are optional. 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 extents 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).

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 Plain 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 Plain.

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 and EF.DG11 to EF.DG13. 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. The Terminal Authentication Protocol is outside the scope or 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 Plain 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 Plain.

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 Plain 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].

3.3 Threats

The Security Target Lite EP-COS V3.0 Plain 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 Plain. The list of threats is included as they are applicable without any changes compared to [19].

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

3.4 Organizational Security Policies

The Security Target Lite EP-COS V3.0 Plain 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 Plain. 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 Plain 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 Plain. 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].

4.2 Security Objectives for the Operational Environment

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

OE.MRTD_Manufact **Protection of the MRTD Manufacturing**

OE.MRTD_Deliver **Protection of the MRTD delivery**

OE.Personalization **Personalization of logical MRTD**

OE.Pass_Auth_Sign **Authentication of logical MRTD by Signature**

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

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

OE.Exam_MRTD	**Examination of the MRTD passport book**
OE.Passive_Auth_Verif	**Verification by Passive Authentication**
OE.Prot_Logical_MRTD	**Protection of data from the logical MRTD**

.

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.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.Passive_Auth_Verif	OE.BAC-Keys	OE.Exam_MRTD	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.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		

The detailed justification for the OSPs and the threats defined in the Protection Profile [19] is already provided in this Protection Profile.

5. Extended Components Definition

This Security Target Lite EP-COS V3.0 Plain 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 Plain.

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 "*list of subjects*" is exchanged by "*authorized user*" and the assignment "*type of persistent memory*" is fixed to "*audit records*". 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].

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 Plain.

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.

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 Plain 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 Plain 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 Plain 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[1] with the capability to store the IC Identification Data [2] 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 [3] and specified cryptographic key sizes 112 bit[4] that meet the following: [8], normative appendix 5[5].

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[6] that meets the following: none[7].

[1] [assignment: *authorised users*]

[2] [assignment: *list of audit information*]

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

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

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

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

[7] [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 [8] in accordance with a specified cryptographic algorithm SHA-1 [9] [10] and cryptographic key sizes none [11] that meet the following: FIPS 180-4 [12] [13].

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 [14] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode [15] and cryptographic key sizes 112 bit [16] that meet the following: FIPS 46-3 [13] and [8]; normative appendix 5, A5.3 [17].

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

[8] [assignment: *list of cryptographic operations*]
[9] [selection: *SHA-1 or other approved algorithms*]
[10] [assignment: *cryptographic algorithm*]
[11] [assignment: *cryptographic key sizes*]
[12] [selection: *FIPS 180-4 or other approved standards*]
[13] [assignment: *list of standards*]
[14] [assignment: *list of cryptographic operations*]
[15] [assignment: *cryptographic algorithm*]
[16] [assignment: *cryptographic key sizes*]
[17] [assignment: *list of standards*]

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

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 [22] in accordance with a specified cryptographic algorithm Triple-DES[23] and cryptographic key sizes 112 bit[24] that meet the following: FIPS 46-3 [13][25].

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

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 [26] (as defined in [7])

6.1.3 Class FIA Identification and Authentication

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

[18] [assignment: *list of cryptographic operations*]
[19] [assignment: *cryptographic algorithm*]
[20] [assignment: *cryptographic key sizes*]
[21] [assignment: *list of standards*]
[22] [assignment: *list of cryptographic operations*]
[23] [assignment: *cryptographic algorithm*]
[24] [assignment: *cryptographic key sizes*]
[25] [assignment: *list of standards*]
[26] [assignment: *additional test suites*]

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)

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”[27]

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

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

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”[28]

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.

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

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

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[29].

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[30]

to support user authentication.

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

1. the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s) the 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 [31].

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[32].

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

[30] [assignment: *list of multiple authentication mechanisms*]

[31] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

[32] [assignment: *list of conditions under which re-authentication is required*]

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[33] unsuccessful authentication attempts occur related to events in column 2 of Table 5[34].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[35], the TSF shall return an action defined in column 3 of Table 5[36].

Table 5. Operations performed in FIA_AFL.1

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
10	Unsuccessful authentication attempt with Document Basic Access MAC Key (K_{MAC}) as Basic Inspection System for the first command of a session (cf. FIA_UAU.5)	After 10 unsuccessful authentication attempt a power-on reset is need to restart the device
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

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 Subset access control – Basic Access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

[34] [assignment: *list of authentication events*]

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

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

FDP_ACC.1.1	The TSF shall enforce the Basic Access Control SFP [37] on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD [38].

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.

6.1.4.2 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 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	The TSF shall enforce the Basic Access Control SFP[39] to objects based on the following: 1. Subjects: a. Personalization Agent, b. Basic Inspection System, c. Terminal, 2. Objects: a. data EF.DG1 to EF.DG16 of the logical MRTD, b. data in EF.COM, c. data in EF.SOD, 3. Security attributes a. authentication status of terminals [40].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: 1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD, 2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD [41].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[42].

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

[38] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

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

[40] [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*]

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

[42] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

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

1. Any Terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.
2. Any Terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.
3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4[43].

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[44] to be able to transmit and receive[45] 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 [46] to be able to transmit and receive [47] user data in a manner protected from modification, deletion, insertion and replay [48] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay [49] has occurred.

[43] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

[44] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[45] [selection: *transmit, receive*]

[46] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[47] [selection: *transmit, receive*]

[48] [selection: *modification, deletion, insertion, replay*]

[49] [selection: *modification, deletion, insertion, replay*]

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 [50].

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 [51].

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.

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.

[50] [assignment: *list of management functions to be provided by the TSF*]

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

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 [52] the Initialization Data and Pre-personalization Data [53] to the Manufacturer [54].

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 [55] the Initialization Data [56] to the Personalization Agent [57].

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 [58] the Document Basic Access Keys [59] to the Personalization Agent [60].

FMT_MTD.1/KEY_READ Management of TSF data – Key Read

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

[53] [assignment: *list of TSF data*]

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

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

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

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

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

[59] [assignment: *list of TSF data*]

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

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 [61] the Document Basic Access Keys and Personalization Agent Keys [62] to none[63].

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[64] in excess of non useful information [65] enabling access to Personalization Agent Key(s) and **Document Basic Access Keys**[66] and EF.COM, EF.SOD, EF.DG1, EF.DG2, and EF.DG6 to EF.DG14 and EF.DG16[67].
FPT_EMS.1.2	The TSF shall ensure any unauthorized users [68] are unable to use the following interface smart card circuit contacts [69] to gain access to Personalization Agent Key(s) and **Document Basic Access Keys**[70] and, EF.COM, EF.SOD, EF.DG1, EF.DG2, and EF.DG6 to EF.DG14 and EF.DG16[71].

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.

[61] [selection: *change_default, query, modify, delete, clear,* [assignment*: other operations*]]
[62] [assignment: *list of TSF data*]
[63] [assignment: *the authorised identified roles*]
[64] [assignment: *types of emissions*]
[65] [assignment: *specified limits*]
[66] [assignment: *list of types of TSF data*]
[67] [assignment: *list of types of user data*]
[68] [assignment: *type of users*]
[69] [assignment: *type of connection*]
[70] [assignment: *list of types of TSF data*]
[71] [assignment: *list of types of user data*]

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 [72].

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[73] to demonstrate the correct operation of the TSF[74].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data[75].

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.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing [76] to the TSF [77] 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.

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

[73] [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]*]

[74] [selection: [assignment: *parts of TSF*], *the TSF*]

[75] [selection: [assignment: *parts of TSF*], *TSF data*]

[76] [assignment: *physical tampering scenarios*]

[77] [assignment: *list of TSF devices/elements*]

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
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_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					
FDP_ACC.1	x	x	x					
FDP_ACF.1	x	x	x					
FDP_UCT.1	x	x	x					
FDP_UIT.1	x	x	x					
FMT_SMF.1	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					
FMT_MTD.1/KEY_READ	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.

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 7 shows the dependencies between the SFR of the TOE.

Table 7. 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

SFR	Dependencies	Support of the 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
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.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1, 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
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
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
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

SFR	Dependencies	Support of the Dependencies
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 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.

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 Plain. 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.

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 unlocked 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.

Personalization of the TOE including writing the Basic Access Control keys is controlled by the access control policy defined by FDP_ACC.1 and FDP_ACF.1.

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.

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 several unsuccessful authentication attempts of the Basic Inspection System. The TOE delays authentication attempts by forcing 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. 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 and FDP_ACF.1.

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 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

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".

7.1 Compatibility

This composite Security Target Lite EP-COS V3.0 Plain 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 8. 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)	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												
FCS_COP.1/SHA								X				
FCS_COP.1/ENC							X					
FCS_COP.1/AUTH							X					
FCS_COP.1/MAC							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 9. Acronyms

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

9. Literature

Common Criteria

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

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

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

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

[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, 25th March 2009

Security Targets

[20] Security Target NXP Secure Smart Card Controller P6021y VB, Rev. 1.11, 23 August 2019 under reference BSI-DSZ-CC-1072

[21] Security Target Crypto Library V3.1.x on P6021y VB, Rev. 1.9, 22 March 2018, under reference NSCIB-CC-15-66030-CR5

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 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

No table of figures entries found.

12. List of tables

13. Contents

Date of release: 07 February 2022
Document identifier: 408325