Security Target Mercury ePassport v1.16

Revision: 2.0

Table of Contents

1 Security Target Introduction (ASE_INT)

1.1 ST reference

The title of this document is “Security Target Mercury ePassport v1.16,”. It´s version is 2.0 dated 2017-01-13.

1.2 TOE reference

The TOE is a composite based on the M7892 D11 platform (for details see [ST_Platform]). The name of the TOE is Mercury ePassport v1.16. The TOE is a contactless chip implementing an ePassport and its version is v1.16.

This ST is compatible to [ST_Platform]. It is strictly conformant to [PP_SAC], if a BIS chooses PACE as authentication method and [PP_BAC], if a BIS chooses BAC as authentication method.

In order to identify the TOE a functionality is provided to the personalization agent to extract the hash values (CBC MAC according to [ISO9797-1] MAC algorithm 1 with key value zero) over several TOE components.The TOE can be identified by the hash references as follows:

Table 1 Hash values

TOE component	Hash value
Mercury ePassport application	`afe6cd4c5de77b1d03d6315c11a3cbbe`
Mercury OS	`c64640b66754c86185cbe70b274e193f`
Mercury pre-personalized file system	`466d5bc7f87e18d513104a2832b28fba`
Hardware identification data	`7633A301254EA097A6D57CFE3BD53A19`

The Mercury OS version is 2016.09.

1.3 TOE overview

1.3.1 TOE definition

The Target of Evaluation (TOE) addressed by this ST is an electronic travel document representing a contactless smart card programmed according to [ICAO_SAC]. This smart card / passport provides the following application:

- the travel document containing the related user data as well as data needed for authentication (incl. PACE/BAC passwords); this application is intended to be used by governmental organisations as a machine readable travel document (MRTD).

For the ePassport application, the travel document holder can control access to his user data by conscious presenting his travel document to governmental organisations.The travel document’s chip is integrated into a physical (plastic or paper), optically readable part of the travel document, which – as the final product – shall eventually supersede still existing, merely optically readable travel documents. The plastic or paper, optically readable cover of the travel document, where the travel document’s chip is embedded in, is not part of the TOE. The tying-up of the travel document’s chip to the plastic travel document is achieved by physical and organizational security measures being out of scope of the TOE.

1.3.2 TOE operational usage

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this ST contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods (see [ICAO_9303_01]) in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the traveler is based on the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page. The issuing State or Organization is supposed to verify the authenticity of the data of genuine MRTD's. The receiving State is supposed to trust a genuine MRTD of an issuing State or Organization.

1.3.3 TOE major security features

The following TOE security features are the most significant for its operational use:

- Only terminals possessing authorisation information (the shared secret MRZ optically retrieved by the terminal) can get access to the user data stored on the TOE and use security functionality of the travel document under control of the travel document holder,
- Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the terminal connected
- Averting of inconspicuous tracing of the travel document,
- Self-protection of the TOE security functionality and the data stored inside.

The authentication mechansisms in operation mode contributing to a Security Function are PACE and BAC. Any product using BAC will be conformant to [PP_BAC] but not to [PP_SAC]. Conversely any product using PACE will be conformant to [PP_SAC] but not to [PP_BAC]; i.e. the TOE supports BAC, but, while performing BAC, it is acting outside of security policy defined by the [PP_SAC]. Therefore, organizations being responsible for the operation of inspection systems shall be aware of this context.

1.4 TOE Description

1.4.1 Component overview

Figure 1 provides an overview of the TOE's components:

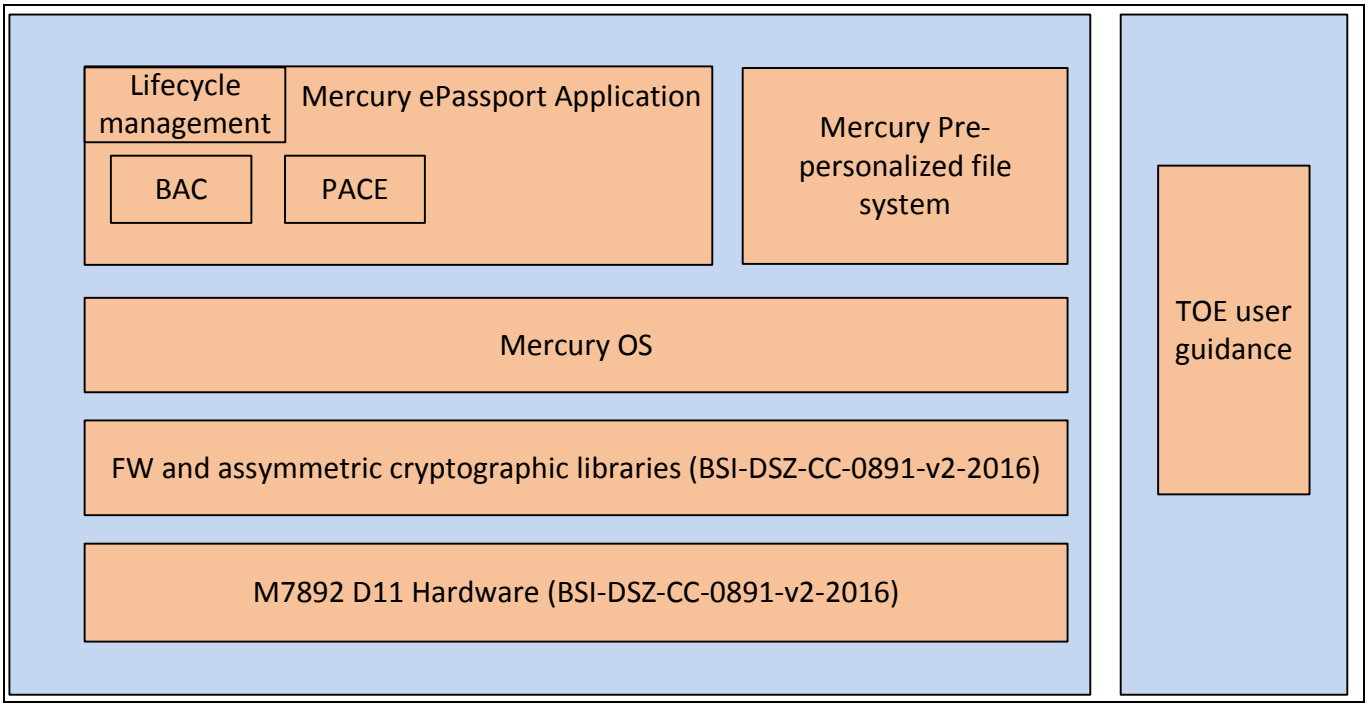

Figure 1 TOE components overview

The TOE is a contactless chip of an ePassport including the Mercury ePass application. It is based on the requirements from the ICAO for machine readable travel documents, i.e. [ICAO_9303_10] and [ICAO_9303_11]. It follows the requirements from [TR-03110_1], [TR-03110_2] and [TR-03110_3]. The authentication schemes as follows are implemented:

- BAC mutual authentication scheme with session key agreement according to [ICAO_9303_11]
- PACE mutual authentication scheme with session key agreement according to [ICAO_9303_11]

The authentication mechansisms in operation mode contributing to a Security Function are PACE and BAC. Any product using BAC will be conformant to [PP_BAC] but not to [PP_SAC]. Conversely any product using PACE will be conformant to [PP_SAC] but not to [PP_BAC]; i.e. the TOE supports BAC, but, while performing BAC, it is acting outside of security policy defined by the [PP_SAC]. Therefore, organizations being responsible for the operation of inspection systems shall be aware of this context.

The security IC hardware is a M7892 D11 device certified under BSI-DSZ-CC-0891-v2-2016. It also contains firmware and asymmetric cryptographic libraries (ACL). Table 2 describes the platform configuration used for this TOE

Table 2 Platform Configuration

Module / Feature	Values
Memories	
SOLID FLASH™ NVM	404k
RAM	8k
Modules	
Crypto2304T	Available
SCP	Available
Interfaces	

Security Target Introduction (ASE_INT)

Module / Feature	Values
ISO 7816-3 slave	Available
RFI – ISO 14443 generally	Available
ISO 14443 Type B card mode	Available
ISO 18092 NFC passive mode	Available
Mifare hardware support for card mode	Not available
SW support for Mifare compatible 4k cards	Not available
SW support for Mifare compatible 1k cards	Not available
FW	78.015.18.2
ACL	2.03.008

The hardware platform provides effective protection mechanisms against FA. The memories are fully encrypted. The platform contains hardware co-processors, which support cryptographic standards such as TDES, AES and EC. The hardware co-processor SCP has integrated measures against successful SCA. A hardware selftest of security functionality is available and called during startup of the Mercury OS.

The firmware (FW) package is not security relevant and from functional perspective transparent for the user. The ACL offers functionality for EC calculations and uses one of the hardware co-processors. It implements effective measures against successful SCA and FA.

The OS called “Mercury OS” offers hardware platform independent services for

- Memory and storage management
- Crypto operations (hash, EC, TDES and AES)
- Communication via the contactless interface
- Device control management services via a hardware abstraction layer

The Mercury ePassport Application is a native code application, which uses the services of the OS, where available. It manages the various stages of the product’s lifecycle once the application is flashed onto the hardware up to its end of life. The application implements the BAC and PACE protocols. It does not implement any cryptographic primitives, as these are provided by the Mercury OS. Further it manages file access control and authentication failure handling. Also the application controls the secure messaging including error handling using the Mercury OS Crypto services, which subsequently uses the hardware co-processor SCP.The pre-personalised file system contains empty LDS EFs. It does not contain EF.DG3 and EF.DG4. In delivery state the personalization agent key is already stored. The user is blocked from creating or deleting files. In order to personalize the LDS EFs, the user has to perform authentication with the personalization agent key.

The pre-personalized file system consists of empty LDS EFs, ready to be personalized. It does not implement any security mechanisms. Access to the pre-personalized file system is controlled by the Mercury application.

The TOE user guidance comprises:

- [Databook] section 10 “Interface”, which describes the user interfaces including a description of all parameters, output messages and error handling.
- [UserGuide], which provides guidance, how to maintain the targeted security level during personalization and operation phase.

1.4.2 Logical Scope of the TOE

The logical scope of the TOE consists of the elements as follows:

- Mecury OS
- Mercury ePassport application
- Mercury pre-personalized file system

1.4.3 Physical Scope of the TOE

The physical scope of the TOE consists of the elements:

- M7892 D11 Hardware (BSI-DSZ-CC-0891-v2-2016) including firmware and ACL, programmed with the Mercury OS and Mercury ePassport application and a pre-personalized file system
- TOE user guidance

1.4.4 Interfaces of the TOE

- The physical interface of the TOE to the external environment is the entire surface of the IC.
- The RF interface (radio frequency power and signal interface) enables contactless communication between a PICC (proximity integration chip card, PICC) and a terminal reader/writer (proximity coupling device, terminal). The transmission protocol meets [ISO/IEC 14443-3] and [ISO/IEC 14443-4] Type B.
- The command interface to the TOE is provided by the ePassport Application.
- The contact based interface ISO 7816-3. This interface is physically present, however it is not used by the application and not accessible by the user.

1.4.5 Lifecycle and Delivery

The [PP_SAC] and [PP_BAC] define the lifecycle phases for the TOE as follows:

1. Development
   - Step1: Development of hardware and IC dedicated software (firmware)
   - Step2: Development of IC embedded software
2. Manufacturing
   - Step3: manufacturing of IC and IC dedicated software. As the TOE does not provide any user ROM, manufacturing of IC embedded software parts in ROM are not relevant here.
   - Step4 (optional): Combination of IC with contactless interface of the travel document
   - Step5: addition of IC embedded software, creation of ePassport application and addition of pre-personalisation data
3. Personalisation of Travel Document
   - Step6: this step includes e.g personalization of biometric data, configuration of the TSF if necessary
4. Operational Use

- Step7: usage of the TOE by the traveler

The lifecycle of this TOE includes Step1 to Step5. Step1, Step3, Step4 and part of Step5 (addition of IC embedded software) are already covered by the platform certificate **BSI-DSZ-CC-0891-v2-2016**. This evaluation considers Step 2 and subset of Step 5 (creation of ePassport application and addition of pre-personalisation data). Before delivery the TOE is secured with a personalization key. In order to perform personalization and subsequently set the TOE in operation mode authentication with an external subject is required based on the personalization key.

2 Conformance Claims (ASE_CCL)

2.1 CC Conformance Claim

This Security Target and the TOE is Common Criteria version v3.1 part 2 [CCPart2] extended and Common Criteria version v3.1 part 3 [CCPart3] conformant.

2.2 PP Claim

This TOE is strictly conformant to [PP_SAC], if a BIS chooses PACE as authentication method and [PP_BAC], if a BIS chooses BAC as authentication method.

2.3 Package Claim

The assurance level for the TOE is EAL5 augmented with the components ALC_DVS.2 and AVA_VAN.5 in case PACE is chosen as authentication method whereby conformany to [PP_SAC] is claimed. This claim is further referred to as AssuranceLevelSAC.

The assurance level for the TOE is EAL4 augmented with the components ALC_DVS.2 in case BAC is chosen as authentication method whereby conformany to [PP_BAC] is claimed. This claim is further referred to as AssuranceLevelBAC.

3 Security Problem Definition (ASE_SPD)

All assets, subjects and external entities, threats, organisational security policies and assumptions from [PP_SAC] and [PP_BAC] section 3 “Security Problem Definition” are applicable for this TOE.

4 Security Objectives (ASE_OBJ)

All Security Objectives provided by the TOE or by the operational environment as well as the security objectives rationale from [PP_SAC] and [PP_BAC] section 4 “Security Objectives” are applicable for this TOE.

5 Extended Components Definition (ASE_ECD)

[PP_SAC] and [PP_BAC] section 5 “Extended Components Definition” are applicable for this TOE.

6 Security Requirements (ASE_REQ)

6.1 TOE Security Functional Requirements

The security functional requirements (SFR) for this TOE are defined in this chapter.

Table 4 lists all SFRs used for this ST defined in [PP_SAC] and [PP_BAC] and refinements, if available. Some of the SFRs appear in both [PP_SAC] and [PP_BAC] with same name but different content. In such cases the SFR is iterated with either the extension …/BAC or …/PACE.:

Table 3 TOE SFRs equivalent from both [PP_SAC] and [PP_BAC]

FCS_CKM.4	Not refined
FCS_RND.1	Not refined
FMT_MTD.1/INI_ENA	Not refined
FPT_TST.1	Not refined
FPT_PHP.3	Not refined

Table 4 TOE SFRs specifically from [PP_SAC]

TOE SFRs specifically from [PP_SAC]	
FCS_CKM.1/DH_PACE	Not refined
FCS_COP.1/PACE_ENC	Not refined
FCS_COP.1/PACE_MAC	Not refined
FIA_AFL.1/PACE	Not refined
FIA_UID.1/PACE	Not refined
FIA_UAU.1/PACE	Not refined
FIA_UAU.4/PACE	Not refined
FIA_UAU.5/PACE	refined
FIA_UAU.6/PACE	Not refined
FDP_ACC.1/TRM	Not refined
FDP_ACF.1/TRM	refined
FDP_RIP.1	Not refined
FDP_UCT.1/TRM	Not refined
FDP_UIT.1/TRM	Not refined
FTP_ITC.1/PACE	refined (by [PP_SAC])
FAU_SAS.1	Not refined
FMT_SMF.1	Not refined
FMT_SMR.1/PACE	Not refined
FMT_LIM.1	Not refined

Security Requirements (ASE_REQ)

TOE SFRs specifically from [PP_SAC]	
FMT_LIM.2	Not refined
FMT_MTD.1/INI_DIS	Not refined
FMT_MTD.1/KEY_READ	Not refined
FMT_MTD.1/PA	Not refined
FPT_EMS.1	Not refined
FPT_FLS.1	Not refined

Table 5 TOE SFRs specifically from [PP_BAC]

TOE SFRs specifically from [PP_BAC]	
FCS_CKM.1	Not refined
FCS_COP.1/SHA	Not refined
FCS_COP.1/ENC	Not refined
FCS_COP.1/AUTH	Not refined
FCS_COP.1/MAC	Not refined
FIA_UID.1	Not refined
FIA_UAU.1	Not refined
FIA_UAU.4	Not refined
FIA_UAU.5	Not refined
FIA_UAU.6	Not refined
FIA_AFL.1	Not refined
FDP_ACC.1	Not refined
FDP_ACF.1	refined
FDP_UCT.1	Not refined
FDP_UIT.1	Not refined
FAU_SAS.1/BAC	Not refined
FMT_SMF.1/BAC	Not refined
FMT_SMR.1	Not refined
FMT_LIM.1/BAC	Not refined
FMT_LIM.2/BAC	Not refined
FMT_MTD.1/INI_DIS/BAC	Not refined
FMT_MTD.1/KEY_WRITE	Not refined
FMT_MTD.1/KEY_READ/BAC	Not refined
FPT_EMSEC.1	Not refined
FPT_FLS.1/BAC	Not refined

There are no refinements available.

6.2 Common SFRs from [PP_BAC] and [PP_SAC]

6.2.1 Class FCS: Cryptographic Support

FCS_CKM.4 Cryptographic key destruction – Session keys

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1 in case of BAC; fulfilled by FCS_CKM.1/DH_PACE in case of PACE

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the key values with random values that meets the following: none

Application Note: Application note 19 of [PP_BAC] and application note 28 of [PP_SAC] are both applicable for this SFR. There is no contradiction between the two application notes. While the application note from [PP_BAC] simply requests the encryption and message authentication keys to be destroyed, the application note from [PP_SAC] provides more detailed requests, when the session keys have to be destroyed. Therefore FCS_CKM.4 from [PP_SAC] and [PP_BAC] can be combined.

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 Random numbers generation Class PTG.2 according to [AIS31]

Application Note: There is no contradiction between application note 24 of [PP_BAC] and application note 31 of [PP_SAC]. Both application notes shall apply and therefore FCS_RND.1 from [PP_BAC] and [PP_SAC] can be combined, i.e. the random numbers shall be used for the PACE, BAC and the authentication mechanism based on Triple-DES (as defined in FIA_UAU.4/PACE and FIA_UAU.4).

6.2.2 Class FMT Security Management

FMT_MTD.1/INI_ENA Management of TSF data – Writing Initialisation and Pre-personalisation Data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 for PACE; fulfilled by FMT_SMF.1/BAC for BAC

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE for PACE; fulfilled by FMT_SMR.1 for BAC

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

Application Note: The application note 42 of [PP_BAC] applies. This application note provides a definition, what is meant by “Pre-personalization Data”. This definition is also applicable to FMT_MTD.1/INI_ENA from [PP_SAC]. Therefore FMT_MTD.1/INI_ENA from [PP_BAC] and [PP_SAC] can be combined.

6.2.3 Class FPT Protection of the Security Functions

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, to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of the TSF data.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Application Note: There is no contradiction between application note 46 of [PP_BAC] and application note 52 of [PP_SAC]. In fact, although the wording is slightly different, the meaning of these application notes is identical. Therefore either of these application notes applies and FPT_TST.1 from [PP_BAC] and [PP_SAC] can be combined.

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 to the TSF by responding automatically such that the SFRs are always enforced.

Application Note: Application note 47 of [PP_BAC] and 53 of [PP_SAC] are equivalent. Application note 48 of [PP_BAC] is only informative to the reader in the sense, that it provides a context to an older CC standard, but not relevant for the interpretation of FPT_PHP.3. Therefore either application note 47 of [PP_BAC] or application note 53 of [PP_SAC] applies and FPT_PHP.3 from [PP_BAC] and [PP_SAC] can be combined.

6.3 SFRs specifically from [PP_SAC]

6.3.1 Class FCS: Cryptographic Support

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

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]

Justification: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case. FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_CKM.1.1/DH_PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH compliant to [TR_ECC] and specified cryptographic key size Table 6 column key size that meet the following: [ICAO_SAC].

Table 6 FCS_CKM/DH_PACE Key Sizes

Security Requirements (ASE_REQ)

algorithm	Key size
ECDH key agreement algorithm	192, 224, 256, 320, 384, 512, 521
AES session keys	128, 192, 256
TDES session keys	112

FCS_COP.1/PACE_ENC Cryptographic operation – Encryption / Decryption AES / 3DES

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE

FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.

FCS_COP.1.1/PACE_ENC The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm AES and 3DES in CBC mode and cryptographic key sizes 112, 128, 192 and 256 bit that meet the following: compliant to [ICAO_SAC]

Application Note: 3DES in CBC mode is used with key size of 112 bit. AES in CBC mode is used with key size of 128, 192 or 256 bit. The TOE implements the cryptographic primitives (i.e. Triple-DES and AES) for secure messaging with encryption of the transmitted data and encrypting the nonce in the first step of PACE. The keys are agreed between the TOE and the terminal as part of the PACE protocol according to FCS_CKM.1/DH_PACE.

FCS_COP.1/PACE_MAC MAC Cryptographic operation – MAC

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE

FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.

FCS_COP.1.1/PACE_MAC The TSFshall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm CMAC and Retail-MAC and cryptographic key sizes 112, 128, 192, 256 bit that meet the following: compliant to [ICAO_SAC] .

Application Note: In accordance with [ICAO_SAC] the (two-key) Triple-DES (112 Bit) could be used in Retail mode for secure messaging.

6.3.2 Class FIA Identification and Authentication

FIA_AFL.1/PACE Authentication failure handling – PACE authentication using non-blocking authorisation data

Hierarchicalto: No other components.

Security Requirements (ASE_REQ)

Dependencies:	FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE
FIA_AFL.1.1/PACE	The TSF shall detect when one unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password
FIA_AFL.1.2/PACE	When the defined number of unsuccessful authentication attempts has been met, the TSF shall increasingly slow down the performance up to a maximum not higher than 6 seconds verifying the authentication token.

FIA_UID.1/PACE	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1/PACE	The TSF shall allow 1. to establish a communication channel, 2. carry out the PACE Protocol according to [ICAO_SAC] 3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS 4. none on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/PACE	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/PACE	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE
FIA_UAU.1.1/PACE	The TSF shall allow 1. to establish a communication channel, 2. carrying out the PACE Protocol according to [ICAO_SAC] 3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, 4. none on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/PACE	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4/PACE	**Single-use authentication of the Terminals by the TOE**
Hierarchical to:	No other components.

Security Requirements (ASE_REQ)

Dependencies: No dependencies.

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

1. PACE Protocol according to [ICAO_SAC]
2. Authentication Mechanism based on Triple-DES
3. none

FIA_UAU.5/PACE Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/PACE The TSF shall provide

1. PACE Protocol according to [ICAO_SAC] ,
2. Passive Authentication according to [ICAO_9303_1]
3. Secure messaging in MAC-ENC mode according to [ICAO_SAC]
4. Symmetric Authentication Mechanism based on Triple-DES
5. none

to support user authentication.

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

1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.
2. The TOE accepts the authentication attempt as Personalisation Agent by a challenge response protocol by means of Triple-DES using the personalization key
3. none

Refinement: FIA_UAU.5.2/PACE of [PP_SAC] seems to contain a flaw within the second list item. It requests a selection, whereby no selection options are provided. The ST writer assumes, that this should rather be an assignment and refined this SFR by performing an assignment instead of a selection.

FIA_UAU.6/PACE Re-authenticating of Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/PACE The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal.

6.3.3 Class FDP User Data Protection

FDP_ACC.1/TRM Subset access control – Terminal Access

Hierarchical to: No other components.

Security Requirements (ASE_REQ)

Dependencies: FDP_ACF.1 Security attribute based access control: fulfilled by FDP_ACF.1/TRM

FDP_ACC.1.1/TRM The TSF shall enforce the Access Control SFP on terminals gaining access to the User Data stored in the travel document and EF.SOD

Application note: Please note that the Document Security Object (SOD) stored in EF.SOD (see [ICAO_9303_01]) does not belong to the user data, but to the TSF-data. The Document Security Object can be read out by the PACE authenticated BIS-PACE, see [ICAO_9303_01].

FDP_ACF.1/TRM Security attribute based access control – Terminal Access

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1/TRM

FMT_MSA.3 Static attribute initialisation: not fulfilled, but justified

The access control TSF according to FDP_ACF.1/TRM uses security attributes having been defined during the personalisation and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

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

1. Subjects:
   a) Terminal,
   b) BIS-PACE;
2. Objects:
   a) data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 , EF.SOD and EF.COM of the logical travel document
   ~~b) data in EF.DG3 of the logical travel document,~~
   ~~c) data in EF.DG4 of the logical travel document~~
3. Security attributes:
   a) Authentication status of terminals
4. none

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

1. A BIS-PACE is allowed to read data objects from FDP_ACF.1/TRM according to [ICAO_SAC] after a successful PACE authentication as required by FIA_UAU.1/PACE.

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

FDP_ACF.1.4/TRM The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1. Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document.
2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document
3. none

Security Requirements (ASE_REQ)

Refinement: This SFR was refined (deletion of b and c from the list of Objects) as the optional EF.DG3 and EF.DG4 are not created and therefore do not exist.

FDP_RIP.1	**Subset residual information protection**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the following objects: 1. Session Keys (immediately after closing related communication session), 2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret K), 3. none

FDP_UCT.1/TRM	**Basic data exchange confidentiality – MRTD**
Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] fulfilled by FTP_ITC.1/PACE [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/TRM
FDP_UCT.1.1/TRM	The TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/TRM	**Data exchange integrity**
Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] fulfilled by FTP_ITC.1/PACE [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/TRM
FDP_UIT.1.1/TRM	The TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.
FDP_UIT.1.2/TRM	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred.

6.3.4 Class FTP Trusted Path/Channels

FTP_ITC.1/PACE	**Inter-TSF trusted channel after PACE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

Security Requirements (ASE_REQ)

FTP_ITC.1.1/PACE	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/PACE	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/PACE	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Terminal.

6.3.5 Class FAU Security Audit

FAU_SAS.1 Audit storage

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the Manufacturer with the capability to store the Initialisation and Pre-Personalisation Data in the audit records.

6.3.6 Class FMT Security Management

FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSFshall be capable of performing the following management functions: 1. Initialization, 2. Pre-personalisation, 3. Personalisation, 4. Configuration.

FMT_SMR.1/PACE Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE
FMT_SMR.1.1/PACE	The TSFshall maintain the roles 1. Manufacturer, 2. Personalisation Agent, 3. Terminal, 4. PACE authenticated BIS-PACE. 5. none

Security Requirements (ASE_REQ)

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

FMT_LIM.1	**Limited capabilities**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability: fulfilled by FMT_LIM.2
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 do not allow 1. User Data to be manipulated and disclosed, 2. TSF data to be manipulated or disclosed, 3. software to be reconstructed, 4. substantial information about construction of TSF to be gathered which may enable other attacks and 5. none

FMT_LIM.2	**Limited availability**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities: fulfilled by FMT_LIM.
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 do not allow 1. User Data to be manipulated and disclosed, 2. TSF data to be manipulated or disclosed, 3. software to be reconstructed, 4. substantial information about construction of TSF to be gathered which may enable other attacks and 5. none

FMT_MTD.1/INI_DIS personalisation Data	**Management of TSF data – Reading and Using Initialisation and Pre-**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1	Security roles: fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1/INI_DIS	The TSF shall restrict the ability to read out the Initialisation Data and the Pre-personalisation Data to the Personalisation Agent.

Security Requirements (ASE_REQ)

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/KEY_READ TheTSF shall restrict the ability to read the

1. PACE passwords,
2. Personalisation Agent Keys
3. none

to none

FMT_MTD.1/PA **Management of TSF data – Personalisation Agent**

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/PA The TSF shall restrict the ability to write the Document Security Object (SO_D) to the Personalisation Agent.

6.3.7 Class FPT Protection of the Security Functions

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 in excess of none useful information enabling access to

1. PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}),
2. the ephemeral private key ephem-SK_{PICC}-PACE
3. none
   and
4. none

FPT_EMS.1.2 The TSF shall ensure any users are unable to use the following interface travel document's contactless/contact interface and circuit contacts to gain access to

1. PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}),
2. the ephemeral private key ephem-SK_{PICC}-PACE
3. none
   and
4. none

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 operating conditions causing a TOE malfunction, 2. Failure detected by TSF according to FPT_TST.1, 3. none

6.4 SFRs specifically from [PP_BAC]

For the dependencies of the SFRs specifically from [PP_BAC] please refer to [PP_BAC] section 6.3.2 “Dependency Rationale”

6.4.1 Class FCS: Cryptographic Support

FCS_CKM.1 TOE	**Cryptographic key generation – Generation of Document Basic Access Keys by the**
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	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [ICAO_9303_01], normative appendix 5

FCS_COP.1/SHA	**Cryptographic operation – Hash for Key Derivation**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SHA	The TSF shall perform hashing in accordance with a specified cryptographic algorithm SHA-1 and cryptographic key sizes none that meet the following: [NIST_Hash]

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 in accordance with a specified cryptographic algorithm Triple-DES in CBC mode and cryptographic key sizes 112 bit that meet the following: [NIST_DES] and [ICAO_9303_01]; normative appendix 5, A 5.3

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

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 Importof user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
	FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm Retail MAC and cryptographic key sizes 112 bit that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)

6.4.2 Class FIA Identification and Authentication

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” 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.

FIA_UAU.1	**Timing of authentication**

Security Requirements (ASE_REQ)

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” 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.

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

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 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.

FIA_UAU.6 Re-authenticating – Re-authenticating of Terminal by the TOE

Hierarchical to:	No other components.
Dependencies:	No dependencies.

Security Requirements (ASE_REQ)

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.

FIA_AFL.1	**Authentication failure handling**
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when one unsuccessful authentication attempts occur related to authentication attempts using the BAC password as shared password.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met the TSF shall increasingly slow down the performance up to a maximum not higher than 6 seconds verifying the authentication token.

6.4.3 Class FDP User Data Protection

FDP_ACC.1	**Subset access control – Basic Access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the Basic Access Control SFP on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD.

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 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

Security Requirements (ASE_REQ)

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

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

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

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

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

Refinement: This SFR was refined (deletion of 3. from the list of Objects) as the optional EF.DG3 and EF.DG4 are not created and therefore do not exist.

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 to be able to transmit and receive user data in a manner protected from unauthorized disclosure.

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 to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.

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

6.4.4 Class FAU Security Audit

FAU_SAS.1/BAC Audit storage

Hierarchical to: No other components.

Security Requirements (ASE_REQ)

Dependencies:	No dependencies.
FAU_SAS.1.1/BAC	The TSF shall provide the Manufacturer with the capability to store the IC Identification Data in the audit records.

6.4.5 Class FMT Security Management

FMT_SMF.1/BAC	**Specification of Management Functions**
Hierarchical to:	No other components.
Dependencies:	No Dependencies
FMT_SMF.1.1/BAC	The TSF shall be capable of performing the following management functions: 1. Initialization, 2. Pre-personalization, 3. Personalization.
FMT_SMR.1	**Security roles**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE
FMT_SMR.1.1	The TSF shall maintain the roles 1. Manufacturer, 2. Personalization Agent, 3. Basic Inspection System
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

FMT_LIM.1/BAC	**Limited capabilities**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability: fulfilled by FMT_LIM.2
FMT_LIM.1.1 /BAC	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 do 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

FMT_LIM.2/BAC	**Limited availability**
Hierarchical to:	No other components.

Security Requirements (ASE_REQ)

Dependencies: FMT_LIM.1 Limited capabilities: fulfilled by FMT_LIM.

FMT_LIM.2.1/BAC 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 do 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

FMT_MTD.1/INI_DIS/BAC Management of TSF data – Reading and Using Initialisation and Pre-personalization Data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

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

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 the Document Basic Access Keys to the Personalization Agent.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/KEY_READ/BAC TheTSF shall restrict the ability to read the Document Basic Access Keys and Personalization Agent Keys to none

6.4.6 Class FPT Protection of the Security Functions

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No Dependencies.

Security Requirements (ASE_REQ)

FPT_EMSEC.1.1	The TOE shall not emit electromagnetic and current emissions in excess of none useful information enabling access to Personalization Agent Key(s) and Document Basic Access Keys
FPT_EMSEC.1.2	The TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Key(s) and Document Basic Access Keys.

FPT_FLS.1/BAC **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,

6.5 Security Assurance Requirements for the TOE

The evaluation assurance level is EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5 with respect to all SFRs from chapter 6.2 and chapter 6.3 and EAL 4 augmented with ALC_DVS.2 with respect to all SFRs from chapter 6.4. The assurance classes and EAL packages are defined in [CCPart3].

Due to the different assurance levels claimed within this ST, the SFRs are ordered according to their respective assurance targets. For all SFRs, which appear in both [PP_SAC] and [PP_BAC] and are equivalent, the assurance requirements AssuranceLevelSAC are applicable. This is because the assurance requirements AssuranceLevelSAC are hierarchical to the assurance requirements AssuranceLevelBAC. For all other SFRs from [PP_SAC] the assurance requirements AssuranceLevelSAC are applicable. For all other SFRs from [PP_BAC] the assurance requirements AssuranceLevelBAC are applicable.

6.6 Security Requirements Rational

6.6.1 Security Functional Requirements Rationale

[PP_SAC] and [PP_BAC] section 6.3.1 “Security Functional Requirements Rationale” are also applicable for this chapter.

6.6.2 Rationale for SFR’s Dependencies

[PP_SAC] and [PP_BAC] section 6.3.2 “Rationale for SFR’s Dependencies” are also applicable for this chapter.

6.6.3 Security Assurance Requirements Rationale

[PP_BAC] section 6.3.3 “Security Assurance Requirements Rationale “ is also applicable for this chapter.

[PP_SAC] section 6.3.3 “Security Assurance Requirements Rationale “ is also applicable for this chapter with one additional rationale justifying the security assurance dependencies: With the exception of ALC_DVS.2 and

AVA_VAN.5, all assurance components are part of the EAL5 package, which by package design does not have any dependency conflicts and is hierarchical to EAL4. The assurance components ALC_DVS.2 and AVA_VAN.5 are also part of the assurance requirements from [PP_SAC], where assurance dependencies are met as is shown in section 6.3.3 from [PP_SAC].

EAL5+ augmented with ALC_DVS.2 and AVA_VAN.5 is appropriate for this TOE, because this assurance level is requested by several states. The assurance expectations for this kind of application are high due to the sensitivity of data stored by the TOE. Therefore several governmental organizations request for an increased assurance level.

6.6.4 Security Requirements – Internal Consistency

The rationale for the internal consistency of the SFRs from [PP_SAC] and [PP_BAC] section 6.3.4 “Security Requirements – Internal Consistency” are also applicable to this chapter

The assurance package EAL5 and EAL4 are pre-defined sets of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in [PP_SAC] and [PP_BAC] section 6.6.3 “Security Assurance Requirements Rationale” together with the additional rational from section 6.6.3 show that the assurance requirements are internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

The rationale for internal consistency between functional and assurance requirements from [PP_SAC] and [PP_BAC] section 6.3.4 “Security Requirements – Internal Consistency” are also applicable to this chapter.

6.7 Statement of Compatibility

6.7.1 Classification of Platform TSFs

The TOE indirectly depends on following platform TSFs from [ST_Platform] to meet its additional SFR requirements:

SF_DPM, SF_PS, SF_PMA, SF_CS

provides a mapping of additional TOE SFRs and indirect contribution of platform TSFs:

Table 7 indirect contribution of platform TSFs

Additional TOE SFRs	Contribution of
FCS_CKM.4	SF_CS
FCS_RND.1	SF_CS
FMT_MTD.1/INI_ENA	SF_DPM
FPT_TST.1	SF_PMA
FPT_PHP.3	SF_PMA
FCS_CKM.1/DH_PACE	SF_CS
FCS_COP.1/PACE_ENC	SF_CS
FCS_COP.1/PACE_MAC	SF_CS
FIA_AFL.1/PACE	-
FIA_UID.1/PACE	-
FIA_UAU.1/PACE	-

Security Requirements (ASE_REQ)

FIA_UAU.4/PACE	
FIA_UAU.5/PACE	SF_CS
FIA_UAU.6/PACE	-
FDP_ACC.1/TRM	-
FDP_ACF.1/TRM	-
FDP_RIP.1	SF_PS
FDP_UCT.1/TRM	-
FDP_UIT.1/TRM	-
FTP_ITC.1/PACE	-
FAU_SAS.1	SF_DPM
FMT_SMF.1	-
FMT_SMR.1/PACE	-
FMT_LIM.1	-
FMT_LIM.2	-
FMT_MTD.1/INI_DIS	-
FMT_MTD.1/KEY_READ	-
FMT_MTD.1/PA	-
FPT_EMS.1	SF_PS
FPT_FLS.1	SF_PMA
FCS_CKM.1	SF_CS
FCS_COP.1/SHA	-
FCS_COP.1/ENC	SF_CS
FCS_COP.1/AUTH	SF_CS
FCS_COP.1/MAC	SF_CS
FIA_UID.1	-
FIA_UAU.1	-
FIA_UAU.4	-
FIA_UAU.5	SF_CS
FIA_UAU.6	-
FIA_AFL.1	-
FDP_ACC.1	-
FDP_ACF.1	-
FDP_UCT.1	-
FDP_UIT.1	-
FAU_SAS.1/BAC	SF_DPM
FMT_SMF.1/BAC	-
FMT_SMR.1	-
FMT_LIM.1/BAC	-
FMT_LIM.2/BAC	-

FMT_MTD.1/INI_DIS/BAC	-
FMT_MTD.1/KEY_WRITE	-
FMT_MTD.1/KEY_READ/BAC	-
FPT_EMSEC.1	SF_PS
FPT_FLS.1/BAC	SF_PMA

The TOE relies and is dependent on all SFs except SF_PLA from [ST_Platform].

6.7.2 IP_SFR (Irrelevant Platform SFRs) and RP_SFR (Relevant Platform SFRs) of [ST_Platform]

RP_SFR: FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1, FMT_SMF.1, FCS_COP.1/TDES, FCS_COP.1/AES, FCS_COP.1/ECDH-v2.03.008, FDP_SDI.1, FDP_SDI.2, FRU_FLT.2, FPT_FLS.1, FMT_LIM.1, FMT_LIM.2, FAU_SAS.1, FPT_PHP.3, FDP_ITT.1, FDP_IFC.1, FPT_ITT.1, FDP_SDC.1, FCS_RNG.1, FPT_TST.2, FMT_LIM.1/Loader, FMT_LIM.2/Loader

IP_SFR: FCS_COP.1/RSA-v2.03.008, FCS_CKM.1/RSA-v2.03.008, FCS_COP.1/ECDSA-v2.03.008, FCS_CKM.1/EC-v2.03.008, FCS_COP.1/SHA, FCS_CKM.4/TDES, FCS_COP.1/TDES_SCL, FCS_CKM.4/TDES_SCL, FCS_CKM.4/AES, FCS_COP.1/AES_SCL, FCS_CKM.4/AES_SCL

6.7.3 Compatibility between threats of this ST and[ST_Platform]

- T.Skimming, T.Eavesdropping of [PP_SAC] and [PP_BAC] are specific to MRTDs and they do no conflict with the threats of [ST_Platform].
- T.Tracing of [PP_SAC] and T.Chip_ID of [PP_BAC] are specific to MRTDs and they do not conflict with the threats of [ST_Platform].
- T.Forgery of [PP_SAC] and [PP_BAC] is included in T.Phys-Manipulation of [ST_Platform].
- T.Abuse-Func of [PP_SAC] and [PP_BAC] is included in T.Abuse-Func of [ST_Platform].
- T.Information_Leakage of this ST is included in T.Leak-Inherent and T.Leak-Forced of [ST_Platform].
- T.Phys-Tamper of [PP_SAC] and [PP_BAC] is included in T.Phys-Manipulation of [ST_Platform]
- T.Malfunction of [PP_SAC] and [PP_BAC] is included in T.Malfunction of [ST_Platform].

It can therefore conclude that the threats of this ST and [ST_Platform] are consistent.

6.7.4 Compatibility between security objectives of this ST and [ST_Platform]

The security objectives of this ST are related to [ST_Platform] as follows:

- O.Abuse-Func of [ST_Platform] contributes to OT.Prot_Abuse-Func of [PP_BAC] and [PP_SAC]
- O.Leak-Forced and O.Leak-Inherent of [ST_Platform] contribute to OT.Prot_Inf_Leak of of [PP_BAC] and [PP_SAC]
- O.Phys-Probing, O.Malfunction and O.Phys-Manipulation of [ST_Platform] contribute to OT.Prot_Phys-Tamper of [PP_BAC] and [PP_SAC]
- O.Identification of [ST_Platform] contributes to OT.Identification of [PP_BAC] and [PP_SAC]
- O.Malfunction of [ST_Platform] contributes to OT.Prot_Malfunction of [PP_BAC] and [PP_SAC]
- O.RND, O.TDES and O.AES of [ST_Platform] contributes to OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality of [PP_SAC] and OT.Data_Int and OT.Data_Conf of [PP_BAC]
- OE.Lim_Block_Loader: this objective to the environment of the platform TOE becomes a relevant objective for this TOE and is implicitly contained in OT.Prot_Abuse-Func.

Security Requirements (ASE_REQ)

OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Tracing, OT.AC_Pers from [PP_SAC] are specific to MRTDs and they do not conflict with any security objective from [ST_Platform].

OT.Data_Int, OT.Data_Conf, OT.AC_Pers from [PP_BAC] are specific to MRTDs and they do not conflict with any security objective from [ST_Platform].

The following [ST_Platform] objectives are not relevant for or cannot be mapped to this TOE:

- O.Cap_Avail_Loader: not relevant for this TOE
- O.SHA: the TOE does not utilize any SHA functionality from the platform. The SHA functionality used by the TOE is implemented on composite level.

None of the Security Objectives for the Environment of this ST are linked to the platform and are therefore not applicable to this mapping.

It can be concluded, that there is no conflict between security objectives of this ST and [ST_Platform].

6.7.5 Compatibility between OSP of this ST and [ST_Platform]

P.Manufact, P.Pre-Operational, P.Card_PKI, P.Trustworthy_PKI and P.Terminal of [PP_SAC] are specific to the MRTD and they do no conflict with the OSP of [ST_Platform].

P.Manufact, P.Personalization and P.Personal_Data of [PP_BAC] are specific to the MRTD and they do not conflict with the OSP of [ST_Platform].

The OSP of [ST_Platform] do not conflict with the threats of this ST. The OSP of this ST do not conflict with the threats of [ST_Platform].

It can therefore be concluded that the OSP of this ST and [ST_Platform] are consistent.

6.7.6 Consistency of assumptions

Following table shows the assumptions of [ST_Platform] classified according to [CompositeEvaluation] ASE_COMP.1-9 (IrPA, CfPA or SgPA):

Table 8 Classification of platform assumptions

assumption	classifying	comment
A.Process-Sec-IC	SgPA	This assumption is partly fulfilled by the TOE. Therefore it is classified as significant assumption. The TOE covers the lifecycle stages as defined in section 1.4.5, but not phase 6 and phase 7 from [PP_0084] section 1.2.3 “TOE life cycle”.
A.Resp-Appl	CfPA	This assumption maps to the security objectives OT.Data_Integrity, OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper
A.Key-Function	CfPA	This assumption maps to the security objective OT.Prot_Inf_Leak

This ST does not make any assumptions about the platform. A.Passive_Auth from [PP_SAC] is an assumption specific to MRTDs and does not conflict with the assumptions from [ST_Platform].

A.MRTD_Delivery from [PP_BAC] is related to A.Process-Sec-IC. Whereas A.MRTD_Delivery only covers a subset of lifecycle stages compared to A.Process-Sec-IC, they both focus on protection during delivery to maintain the security goals. There is no contradiction between these assumptions.

Security Requirements (ASE_REQ)

A.Pers_Agent from [PP_BAC] contains assumptions specific to MRTD personalization. It does not contradict A.Process-Sec-IC, which also covers personalization phase, but its focus is on delivery and storage process.

A.MRTD_Manufact, A.Insp_Sys and A.BAC-Keys are assumptions specific to MRTDs and do not conflict with the assumptions from [ST_Platform].

It can therefore be concluded that the assumptions for the environment of this ST and [ST_Platform] are consistent.

7 TOE Summary Specification

This TOE summary specification also draws on the security services provided by the platform product. For a description of these services please refer to [ST_Platform].

The composite TOE provides the security functions as follows:

- **SF_PACE_BAC**

The TOE implements the PACE and BAC protocol (PICC side). It encompasses:

  - ECDH key generation, **FCS_CKM.1/DH_PACE** (SAC): The TOE uses the platform service “Elliptic Curves EC”
  - Generation of Document Basic Access Keys, **FCS_CKM.1** (BAC), **FCS_COP.1/SHA** (BAC): The TOE uses the hardware accelerator SCP (Symmetric Crypto Processor)
  - Key destruction, **FCS_CKM.4**: The TOE uses the platform service “PTRNG respectively TRNG” to destroy keys by overwrite with random values.
  - Provision of random numbers, **FCS_RND.1**: The TOE uses the platform service “PTRNG respectively TRNG”. Authentication failure handling, **FIA_AFL.1/PACE** (SAC)**, FIA_AFL.1** (BAC): The TOE implements this check in such a way, that it withstands tearing events. A counter for unsuccessful authentication attempts is incremented before authentication is performed and reset in case of successful authentication.
  - Prevention of replay attacks, **FIA_UAU.4/PACE** (SAC), **FIA_UAU.4** (BAC): Replay attacks are prevented by the cryptographic protocol, which relies on good quality random numbers as required by FCS_RND.1
  - Multiple authentication, **FIA_UAU.5/PACE** (SAC), **FIA_UAU.5** (BAC): The TOE follows the protocol as described in [ICAO_SAC]
- **SF_AuthPersoAgent**
  - Multiple authentication, **FIA_UAU.5/PACE** (SAC), **FIA_UAU.5** (BAC): The TOE follows the protocol as described in [ICAO_SAC]
  - Cryptographic authentication, F**CS_COP.1/AUTH** (BAC): The TOE uses the hardware accelerator SCP (Symmetric Crypto Processor)
- **SF_SecureMessaging**
  - Secure messaging, encryption/decryption, **FCS_COP.1/PACE_ENC** (SAC)**, FCS_COP.1/ENC** (BAC): The TOE uses the hardware accelerator SCP (Symmetric Crypto Processor)
  - Secure messaging integrity protection, **FCS_COP.1/PACE_MAC** (SAC), **FCS_COP.1/MAC** (BAC): The TOE uses the hardware accelerator SCP (Symmetric Crypto Processor) to calculate CMAC or Retail-MAC.
  - Multiple authentication, **FIA_UAU.5/PACE** (SAC), **FIA_UAU.5** (BAC): The TOE performs a MAC check for every received message before instruction is executed, if the MAC check fails secure messaging is aborted; every response during secure messaging is MAC’ed by the TOE
  - Re-authentication of terminal, **FIA_UAU.6/PACE** (SAC), **FIA_UAU.6** (BAC): The TOE checks for every incoming message, whether the message is genuine (MAC check).
  - Trusted channel, **FTP_ITC.1/PACE** (SAC): The TOE follows the standardized implementation of the trusted channel according to [ICAO_SAC]
- **SF_AccessControl**
  - Allow specific access before user identification, **FIA_UID.1/PACE** (SAC), **FIA_UID.1** (BAC): The access rights information of the TOE grant access to EF.CardAccess (see [ICAO_9303_11]) and EF.ATR/INFO (see [ISO7816-4]) before PACE or BAC authentication is performed. The TOE allows to read a specific subset of initialization data

TOE Summary Specification

- Allow specific access before user authentication, **FIA_UAU.1/PACE** (SAC), **FIA_UAU.1** (BAC): The access rights information of the TOE grant access to EF.CardAccess and EF.ATR/INFO before PACE or BAC authentication was performed. The TOE allows to read a specific subset of initialization data
- Subset and security attribute based access control, **FDP_ACC.1/TRM** (SAC), **FDP_ACC.1** (BAC), **FDP_ACF.1/TRM** (SAC), **FDP_ACF.1** (BAC), the TOE blocks access to EF.SOD, in case BAC or PACE protocol is not successfully performed.
- Residual information protection, **FDP_RIP.1**: as soon scure messaging is stopped, the whole secure messaging context including session keys is wiped with random numbers. The ICC private ECDH key is wiped with random numbers once the secure session key is established.
- Data exchange confidentiality, **FDP_UCT.1/TRM** (SAC), **FDP_UCT.1** (BAC): during secure messaging, responses by the ICC are always wrapped (encrypted and MAC'ed) before being sent.
- Data exchange integrity, **FDP_UIT.1/TRM** (SAC), **FDP_UIT.1** (BAC) : during secure messaging, responses by the ICC are always wrapped (encrypted and MAC'ed) before being sent. A MAC check is performed for each message received during secure messaging.
- Storage of initialization and pre-personalisation data, **FAU_SAS.1** (SAC), **FAU_SAS.1/BAC** (BAC): [PP_BAC] requests storage of IC Identification data, whereas [PP_SAC] requests storage of Initialisation and Pre-Personalisation data, whereby IC Identification data is a subset of Initialisation data. The TOE does not make any distinction, whether BAC or PACE is performed, i.e. stores all of the requested data. The TOE at its stage of delivery (personalization stage) contains a personalization key. The personalization agent has the option to calculate various checksums including software, file system, chip information and lifecycle information.
- Management functions linked to different life cycle states, **FMT_SMF.1** (SAC), **FMT_SMF.1/BAC** (BAC): The management functions "Initialization" and "pre-personalization" are part of the developer lifecycle. In order to write to files within the Mercury ePassport file system in personalization stage, authentication with the personalization agent key has to be performed upfront. [PP_SAC] additionally defines the management function "Configuration". In personalization state the personalization agent has to configure the TOE such, that BAC and/or PACE are active.
- Access is linked to security roles, **FMT_SMR.1/PACE** (SAC), **FMT_SMR.1** (BAC): Access rights are implemented such, that they depend on lifecycle stage and authentication stage (e.g. whether PACE authentication or authentication as personalization agent was successfully performed). Certain commands are blocked during specific lifecycle states, such as the command to read the Initialisation data or update file data in operation state. Read access to specific files is granted or denied depending on the authentication state. Life cycle transition from personalization to operation stage can only be performed by the personalization agent. A back tranisition is blocked.
- Writing of initialization and pre-personalisation data restricted to manufacturer, **FMT_MTD.1/INI_ENA**: during personalization and operation there is no command available to write initialization data (e.g. create files). The command to write the personalization key is not available during personalization or operation phase.
- Reading of initialization and pre-personalisation data restricted to Personalization agent, **FMT_MTD.1/INI_DIS** (SAC) and Disabling of Read Access to Initialization Data to the Personalization agent **FMT_MTD.1/INI_DIS/BAC** (BAC): Althought these two SFRs have slightly different meanings, the TOE generally blocks reading of initialization and pre-personalization data in operation mode. Only the personalization agent is granted to set the lifecycle state from personalization to operation. A back tranisition is blocked.
- Reading of PACE or BAC password and personalization agent key not possible, **FMT_MTD.1/KEY_READ** (SAC), **FMT_MTD.1/KEY_READ/BAC** (BAC): The personalization key is stored in a special key storage within the Mercury OS, which only allows to handle this key by reference; no direct read access is allowed.The PACE or BAC password can only be read, if authenticated with same password.

- Only personalization agent allowed to write Document Security Object (SOD), **FMT_MTD.1/PA**: In operation mode the “UPDATE BINARY” command is blocked.
- Only personalization agent allowed to write Document Basic Access Keys, **FMT_MTD.1/KEY_WRITE** (BAC): in operation stage the proprietary command to write Document Basic Access Keys is blocked.

- **SF_DataProtection**
  - TSF is designed, that it has limited capability and limited availability, **FMT_LIM.1** (SAC), **FMT_LIM.1/BAC** (BAC), **FMT_LIM.2** (SAC), **FMT_LIM.2/BAC** (BAC): in personalization stage only limited test functionality is available. The hash values, which are available to identify the TOE do not allow to retrieve the data it was generated from. In operation stage this test functionality is blocked.
  - sidechannel protection, **FPT_EMS.1** (SAC), **FPT_EMSEC.1** (BAC): The TOE uses the platform service “SF_PS: Protection against Snooping”. Further, authentication attempts as personalization agent are limited. The hardware accelerator SCP is optimized to keep leakage low. For the key generation of the ephemeral private key SK_{PICC}-PACE, the platform service “Elliptic Curves EC” is used, which provides effective measures against leakage attacks.
  - prevention of malfunction, **FPT_FLS.1** (SAC), **FPT_FLS.1/BAC** (BAC): The TOE uses the platform service “SF_PM: Protection against Modifying attacks”. During startup of the Mercury OS a selftest is performed. If this selftest fails a security reset is triggered.
  - self-tests, **FPT_TST.1**: During startup of the Mercury OS the UMSLC (User Mode Security Life Control) selftest offered by the platform is performed. The personalization agent is allowed to retrieve a checksum of the Mercury code.
  - physical protection, **FPT_PHP.3**: The TOE uses the platform services “SF_PS: Protection against Snooping” and “SF_PM: Protection against Modifying attacks”.

8 References

8.1 Literature

[AIS31] Functionality classes and evaluation methodology for physical random number generators AIS31, Version 2.1, 2011-12-02, Bundesamt für Sicherheit in der Informationstechnik.

[CCPart2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements; Version 3.1 Revision 4 Sept 2012, CCMB-2012-09-002

[CCPart3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; Version 3.1 Revision 4 Sept 2012, CCMB-2012-09-003

[CompositeEvaluation] Composite product evaluation for Smart Cards and similar devices, April 2012, Version 1.2, CCDB-2012-04-001

[TR_ECC] Federal Office for Information Security (BSI) TR-03111 Elliptic Curve Cryptography Version 2.0, 2012-06-28

[ICAO_SAC] International Civil Aviation Organization Machine Readable Travel DocumentsTechnical Report Supplemental Access Control for Machine Readable Travel Documents Version 1.00, November 2010

[ICAO_9303_01] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization

[ICAO_9303_10] International Civil Aviation Organization, DOC 9303 Machine Readable Travel Documents Seventh Edition – 2015, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)

[ICAO_9303_11] International Civil Aviation Organization, DOC 9303 Machine Readable Travel Documents Seventh Edition – 2015 Part 11: Security Mechanisms for MRTD's

[ISO9797-1] ISO/IEC International Standard 9797-1:2011-(E), Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechnanisms using a block cipher, Second Edition 2011-03-01

[ISO14443-3] ISO/IEC International Standard 14443-3 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 3: Initialization and anticollisionFirst edition 2001-02-01, AMENDMENT 1: Bit rates of fc/64, fc/32 and fc/16 2005-06-01, ISO/IEC Defect Report and Technical Corrigendum 1 for International 2005-12-16, AMENDMENT 3: Handling of reserved fields and values 2006-03-15

[ISO14443-4] ISO/IEC International Standard 14443-4 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 4: Transmission protocol Second edition 2008-07-15, AMENDMENT 1: Handling of reserved fields and values 2006-03-15

[ISO7816-4] ISO/IEC JTC1/SC17 International Standard 7816-4:2013 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange Date: 2013-04-04

[NIST_Hash] FIPS PUB 180-4, Federal Information Processing Standards Publication Secure Hash Standard (SHS), Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, March 2012

[NIST_DES] FIPS PUB 46-3: Data Encryption Standard (DES), Reaffirmed, 1999 October 25

References

[Databook] Mercury: ePassport Data Book, V1.25, 2016-11-29

[UserGuide] Infineon Technologies Mercury ePassport User Guide, v2.3, 2016-12-13

[ST_Platform] Security Target BSI-DSZ-CC-0891-V2-2016, Version 1.7, 2016-11-16, Confidential Security Target – M7892 Design Steps D11 and G12, Infineon Technologies AG (confidential document)

[TR-03110_1] Federal Office for Information Security (BSI) Technical Guideline TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token Part 1 - eMRTDs with BAC/PACEv2 and EACv1 Version 2.20, 26. February 2015

[TR_03110_2] Federal Office for Information Security (BSI) Technical Guideline TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token Part 2 - Protocols for electronic IDentification, Authentication and trust Services (eIDAS) Version 2.20, 3. February 2015

[TR_03110_3] Federal Office for Information Security (BSI) Technical Guideline TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token Part 3 - Common Specifications Version 2.20, 3. February 2015

[PP_BAC] BSI-CC-PP-0055, Version 1.10, 25.03.2009

[PP_SAC] BSI-CC-PP-0068-V2-2011-MA-01, Version 1.01, 22.07.2014

[PP_0084] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13.01.2014, BSI-CC-PP-0084-2014

Note that the versions of these documents are listed in the certification report.

9 List of Abbreviations

ACL	Asymmetric Cryptographic library
AES	Advanced Encryption Standard
BIS	Basic Inspection System
BAC	Basic Access Control
CA	Chip Authentication
EC	Elliptic Curve
FA	Fault Attacks
FW	Firmware
IC	Integrated Circuit
ICAO	International Civil Aviation Organisation
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
MRZ	Machine readable zoneOS Operating System
OSP	Organisational Security Policy
PACE	Password Autenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
ROM	Read Only Memory
SCA	Side Channel Analysis
SCP	Symmetric Crypto Processor
ST	Security Target
TA	Terminal Authentication
TDES	Triple Data Encryption Algorithm
TOE	Target of Evaluation
TSF	TOE Security Function

10 Revision History

Major changes since the last revision

Version	Description of change
0.2	Initial draft version
2.0	Final version

Edition 2017-01-13

Published by
Infineon Technologies AG
81726 Munich, Germany

Do you have a question about this document?

Email: erratum@infineon.com

AppNote Number
Document reference

IMPORTANT NOTICE

The information contained in this Security Target is given as a hint for the implementation of the product only and shall in no event be regarded as a description or warranty of a certain functionality, condition or quality of the product. Before implementation of the product, the recipient of this application note must verify any function and other technical information given herein in the real application. Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind (including without limitation warranties of non-infringement of intellectual property rights of any third party) with respect to any and all information given in this Security Target.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.