G+D Mobile Security

STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1

Security Target Lite

Version 1.11

Author : G+D Mobile Security
Status : Final
Rating : Public
File : GDM_STA37_ID_C1_ASE_Lite.docx

Edition : 16.07.2020

Contents

Tables

History of this document

Version	Date	Author	Description
1.11	16.07.20	uta	Final version

1 ST Introduction

1.1 ST Reference

Title: Security Target Lite STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1

Reference: GDM_STA37_ID_C1_ASE_Lite

Version 1.11/Status 16.07.2020

Origin: Giesecke+Devrient Mobile Security GmbH

Author: uta/MSRD34

CC Version: 3.1 (Revision 5)

Assurance Level: EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

TOE: STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1

TOE documentation:

- Guidance Documentation STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1 – Main Document
- Guidance Documentation for the Initialisation Phase STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1
- Guidance Documentation for the Personalisation Phase STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1
- Guidance Documentation for the Usage Phase STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1

HW-Part of TOE: Infineon IFX_CCI_000005h (Certificate: BSI-DSZ-CC-1110-V3-2020). This TOE was evaluated against Common Criteria Version 3.1.

1.2 TOE Overview

This document is the Security Target for STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1. In the following chapters: “STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1” stands for the Target of Evaluation (TOE).

The related products are the STARCOS 3.7 ID ePA C1 Card, the STARCOS 3.7 ID eAT C1 Card and the STARCOS 3.7 ID ePass C1 Card.

The STARCOS 3.7 ID ePA C1 Card, the STARCOS 3.7 ID eAT C1 Card and the STARCOS 3.7 ID ePass C1 Card contain the TOE consisting of the:

- STARCOS 3.7 operation system
- ePA, eAT or ePass applications (the dedicated files for the ePassport, the eID-and the eSign application in a file system, see 1.2.8 for the different configurations of the TOE)
- and depends on the secure IFX chip being certified according to CC EAL6+ [HWST] .

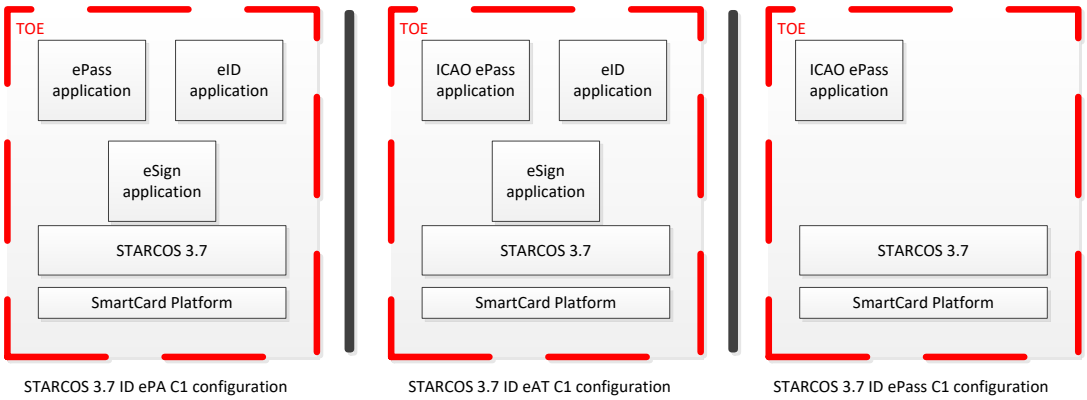

Figure 1: The different TOE configurations

The TOE consists of the related software in combination with the underlying hardware ('Composite Evaluation').

The assurance level for the TOE is CC EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

The TOE can be used in three different configurations defined in 1.2.8.

Up to the personalisation phase the specific TOE configuration can be identified by its response to a specific apdu specified in the Guidance Documentation for the Personalisation Phase.

1.2.1 Sections Overview

Section 1 provides the introductory material for the Security Target.

Section 2 provides the conformance claims for the Security Target.

Section 3 provides a discussion of the security problems for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the operational environment and the security objective rational to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat.

Section 5 contains the extended component definitions.

Section 6 contains the security functional requirements and assurance requirements derived from the Common Criteria [CC1], Part 2 [CC2] and Part 3 [CC3], which are satisfied and the security functional requirements rational. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective.

Section 7 contains the TOE Summary Specification.

Section 8 provides information on used acronyms and glossary and the used references.

1.2.2 TOE definition and operational usage

The Target of Evaluation (TOE) is a smartcard programmed according to [TR03110-1] and [TR03110-2]. The smartcard contains multiple applications. The programmed smartcard is called an electronic document as a whole. Here, an application is a collection of data(groups) and their access conditions. We mainly distinguish between common user data, and sensitive user-data. Depending on the protection mechanisms involved, these user data can further be distinguished as follows:

1. *EAC1-protected data:* Sensitive user data protected by EAC1 (cf. [TR03110-1]),
2. *EAC2-protected data:* Sensitive user data protected by EAC2 (cf. [TR03110-2]), and
3. *all other (common) user data*. Other user data are protected by Password Authenticated Connection Establishment (PACE, cf. also [TR03110-2]). Note that EAC1 recommends, and EAC2 requires prior execution of PACE.

Application Note 1: (from MR.ED2.0) Due to migration periods, there are products that functionally support both PACE and Basic Access Control (BAC), i.e. Supplemental Access Control (SAC) [ICAO9303]. However, any product using BAC is not conformant to [MR.ED2.0]; i.e. this TOE functionally supports BAC, but, while performing BAC, it is acting outside of the security policy defined in this document.

In addition to the above user data, there are also data required for TOE security functionality (TSF). Such data is needed to execute the access control protocols, to verify integrity and authenticity of user data, or to generate cryptographic signatures.

Applications considered in [TR03110-1] and [TR03110-2] are
1. an electronic passport (ePass) application (containing common and EAC1 protected data, and being conformant to [ICAO9303]),
2. an electronic identity (eID) application (containing common and EAC2 protected data), and
3. a signature (eSign) application (protected by EAC2).

A *configuration of the TOE* is a combination of one or several of the above applications together with corresponding common data, sensitive data, and TSF data. The combination of different applications for a product corresponds to loading different data into the EEPROM or flash memory of a smart card. Such a configuration of data groups yields a specific electronic document.

Applications,that is configurations of data groups, are loaded during manufacturing. Requirements on the loader are adapted from the *CC-Package: Package 1: Loader dedicated for usage in secured environment only* from [ICPP].

As mentioned, access to common and sensitive user data is protected by PACE, EAC1, and/or EAC2 (see below). Thus the electronic document holder can control access to her user data either by consciously presenting her electronic document, and/or by consciously entering a secret personal identification number (PIN).

A data group is defined as either sensitive user data protected by EAC1, sensitive user data protected by EAC2, or common user data. Obviously, if a data group is for example defined as sensitive user data protected by EAC1, but is at the same time defined as common user data and thus accessible by just PACE alone, this defeats the whole purpose of protecting it with the advanced security mechanism EAC1 in the first place. However, to ensure compatibility with standards set by the International Civil Aviation Organization (ICAO) for electronic passports, exceptions are acceptable for certain applications. See also Chapter 1.2.7 for details.

The TOE comprises:
1. the circuitry of the chip, including all integrated circuit (IC) dedicated software that is active in the operational phase of the TOE,
2. the IC embedded software, i.e. the operating system,
3. all access mechanisms, associated protocols and corresponding data,
4. one or several applications(the different configurations are listed in 1.2.8), and
5. the associated guidance documentation.

Application Note 2: Since contactless interface parts (e.g. the antenna) may impact specific aspects of vulnerability assessment and are thus relevant for security, such parts are considered as a part of the TOE.

1.2.3 TOE major security features for operational use

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

- only authenticated terminals can get access to the user data stored on the TOE and use security functionality of the electronic document according to the access rights of the terminal,
- the electronic document holder can control access by consciously presenting his electronic document and/or by entering his secret PIN,
- authenticity and integrity of user data can be verified,
- confidentiality of user data in the communication channel between the TOE and the connected terminal is provided,
- inconspicuous tracing of the electronic document is averted,
- its security functionality and the data stored inside are self-protected, and
- digital signatures can be created, in the configurations of the TOE containing an eSign application.
- It allows to update the TOE software during the life-cycle phase *operational use.*

1.2.4 TOE type

The TOE type addressed by the current security target is a smartcard programmed according to [TR03110-1] and [TR03110-2]. The smartcard contains multiple applications. The programmed smartcard is called an electronic document as a whole.

Justification: TOE type definitions of the claimed PPs ([EAC1PP], [EAC2PP], [SSCDPP]) differ slightly. We argue that these differences do not violate consistency:

The TOE type defined both in [EAC1PP] and [EAC2PP] is a smartcard. Whereas [EAC1PP] references [TR03110-1] (and also [ICAO9303] and related ICAO specifications, however [TR03110-1] is fully compatible with those ICAO specifications, and they are mostly listed there for the sake of completeness and the context of use) w.r.t. programming of the card, [TR03110-2] is given as a reference in [EAC2PP]. Reference [TR03110-1] defines the EAC1 protocol, whereas EAC2 is defined in [TR03110-2]. Thus this difference in reference is introduced just due to different applications on the card,that do not contradict each other. The term 'travel document' of [EAC1PP] is here understood in a broader

sense (cf. also Table 1), since the document can also be used in contexts other than just traveling.

Moreover, [TR03110-2-v2.20] is referenced in difference to the claimed PPs. This reference is only needed for the specification of Chip Authentication 3, an upgraded and extended version of Chip Authentication 2. Since the TOE also supports Chip Authentication 2 there is full compatibility; consistency is not violated.

The TOE type definition given in [SSCDPP] is "*a combination of hardware and software configured to securely create, use and manage signature-creation data (SCD)".* The definition of hardware and software in this ST is more specific by explicitly mentioning a smartcard and the software on the card. However the very fundamental purpose of a smartcard is to store data on it in a protected way. Hence, the TOE type definition of this ST is also not inconsistent with the one of [SSCDPP].

The typical life cycle phases for the current TOE type are development, manufacturing, card issuing and operational use. The life cycle phase development includes development of the IC itself and IC embedded software. Manufacturing includes IC manufacturing and smart card manufacturing, and installation of a card operating system. Card issuing includes installation of the smart card applications and their electronic personalization, i. e. tying the application data up to the electronic document holder.

Operational use of the TOE is explicitly in the focus of claimed MR.ED2.0 PP. Nevertheless, some TOE functionality might not be directly accessible to the end-user during operational use. Some single properties of the manufacturing and the card issuing life cycle phases that are significant for the security of the TOE in its operational phase are also considered by the claimed MR.ED2.0 PP. Conformance with this PP requires that all life cycle phases are considered to the extent that is required by the assurance package chosen here for the TOE; c.f. also Chapter 6.2.

The definition of the TOE and its operational usage is the same as in [MR.ED2.0] with one exception: Here, the TOE additionally has the ability to update its TOE software during the life-cycle phase operational use by an update mechanism. The security of this update mechanism is a subject of this ST.

Note that the part of this ST concerned with the update mechanism is only concerned with the mechanism itself and its security. It is assumed that updates must be authorized by a central entity (e.g. some entity in charge of the security of the electronic document, the document issuer,

the manufacturer, the TOE software developer or some other entity) prior application, and supports this process by cryptographic means.

In particular, the updated TOE software is out of scope of this ST. No assumption is made on the quality and security of the update. To make the point, installing a completely flawed TOE software update that creates new security vulnerabilities or deactivates security mechanisms of the original TOE via the update mechanism would be absolutely valid under the assumptions of this ST.

Except for the update mechanism, the TOE is exactly the same as in [MR.ED2.0].

1.2.5 TOE Life Cycle

The TOE life cycle is described in terms of the above mentioned four life cycle phases. Akin to [ICPP], the TOE life-cycle is additionally subdivided into seven steps.

Phase 1: Development

Step 1
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.

Step 2
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 electronic document application(s) 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 is securely delivered to the IC manufacturer. The IC embedded software in the non-volatile programmable memories, the application(s), and the guidance documentation is securely delivered to the electronic document manufacturer.

Phase 2: Manufacturing
Step 3
In a first step, the TOE integrated circuit is produced. The circuit contains the electronic document's chip dedicated software, and the parts of the electronic document's chip embedded software in the non-volatile non-programmable memory (ROM). The IC manufacturer writes IC identification data onto the chip in order to track and control the IC as dedicated electronic document material during IC manufacturing, and during delivery to the electronic document manufacturer. The IC is securely delivered from the IC manufacturer to the electronic document manufacturer. If necessary, the IC manufacturer adds parts of the IC

embedded software in the non-volatile programmable memory, e. g. EEPROM.

Step 4 (optional)
If the electronic document manufacturer delivers a packaged component, the IC is combined with hardware for the contact based or contactless interface.

Step 5
The electronic document manufacturer
1. if necessary, adds the IC embedded software, or parts of it in the non-volatile programmable memories, e. g. EEPROM or FLASH,
2. creates the application(s), and
3. equips the electronic document's chip with pre-personalization data.

Creation of the application(s) implies the creation of the master file (MF), dedicated files (DFs), and elementary files (EFs) according to [ISO7816-4]. How this process is handled internally depends on the IC and IC embedded software.

The pre-personalized electronic document together with the IC identifier is securely delivered from the electronic document manufacturer to the personalization agent. The electronic document manufacturer also provides the relevant parts of the guidance documentation to the personalization agent.

Phase 3: Personalization of the Electronic Document

Step 6
The personalization of the electronic document includes
1. the survey of the electronic document holder’s biographical data,
2. the enrollment of the electronic document holder's biometric reference data, such as a digitized portrait or other biometric reference data,
3. printing the visual readable data onto the physical part of the electronic document, and
4. configuration of the TSF, if necessary.

Configuration of the TSF is performed by the personalization agent and includes, but is not limited to, the creation of the digitized version of the textual, printed data, the digitized version of e.g. a portrait, or a cryptographic signature of a cryptographic hash of the data that are stored on the chip. The personalized electronic document, if required together with appropriate guidance for TOE use, is handed over to the electronic document holder for operational use.

Application Note 3: TSF data are data for the operation of the TOE upon which the enforcement of the SFRs relies [CC1]. Here TSF data include, but are not limited to, the personalization agent's authentication key(s).

Phase 4: Operational Use

Step 7
The chip of the TOE is used by the electronic document and terminals that verify the chip's data during the phase *operational use*. The user data can be read and modified according to the security policy of the issuer.

Application Note 4: This ST considers the first phase and the second phase, i.e. Step 1 up to Step 5, as part of the evaluation. Therefore the TOE delivery is defined to occur, according to CC, after Step 5. Since specific production steps of the second phase are of minor security relevance (e.g. plastic card or booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national body of the issuer or organization. In this case the national body of the issuer is responsible for these specific production steps.
Note that the personalization process and its environment may depend on specific security needs of the issuer. All production, generation and installation procedures after TOE delivery up to the phase *operational use* have to be considered in the product evaluation process under assurance class AGD. Therefore, the security target has to outline how to split up P.Manufact, P.Personalisation and related security objectives into aspects relevant before vs. those relevant after TOE delivery.

Some production steps, e. g. Step 4 in Phase 2 may also take place in the Phase 3.

The TOE delivery takes place after Step 5.

Phase 1 : Development			
	Step 1	IC developer site	IC certification
	Step 2	IC Embedded Software Developer site	IC embedded Software Developer site certification
Phase 2 : Manufacturing			
	Step 3	IC Manufacturer site	IC certification
	Step 4	IC Packaging Manufacturer	IC Packaging Manufacturer site certification
	Step 5	MRTD Manufacturer	Production site certificate
TOE delivery			
Phase 3 : Personalization of the Electronic Document			
	Step 6	Personalization agent	AGD_PRE

Phase 4 : Operational Use			
	Step 7	End user	AGD_OPE

Figure 2: Subject identification for the different lifecycle steps

1.2.6 Non-TOE Hardware/Software/Firmware

In order to be powered up and to communicate with the external world, the TOE needs a terminal (card reader) supporting the communication according to [ISO7816-4] and [ISO14443]; the latter only if the card has a contactless interface. Akin to [TR03110-1] and [TR03110-2] the TOE is able to recognize the following terminal types:

- **PACE terminal**. A PACE terminal is a basic inspection system according to [TR03110-1], [TR03110-2] resp. It performs the standard inspection procedure, i.e PACE followed by Passive Authentication, cf. [TR03110-1]. Afterwards user data are read by the terminal. A PACE terminal is allowed to read only common user data.
- **EAC1 terminal (for the configurations of the TOE containing an ePass application)**. An EAC1 terminal is an extended inspection system according to [TR03110-1]. It performs the advanced inspection procedure ([TR03110-1]) using EAC1, i.e. PACE, then Chip Authentication 1 followed by Passive Authentication, and finally Terminal Authentication 1. Afterwards user data are read by the terminal. An EAC1 terminal is allowed to read both EAC1 protected data, and common user data.
- **EAC2 terminal (for the configurations of the TOE containing an eID application)**. An EAC2 terminal is an extended inspection system performing the general authentication procedure according to [TR03110-2] using EAC2, i.e. PACE, then Terminal Authentication 2 followed by Passive Authentication, and finally Chip Authentication 2. Depending on its authorization level, an EAC2 terminal is allowed to read out some or all EAC2 protected sensitive user data, and common user data.
- **Update terminal.** An update terminal is used to read out version information of the TOE software, read update log data, and to install new TOE software on the TOE.

In general, the authorization level of a terminal is determined by the effective terminal authorization. The authorization is calculated from the certificate chain presented by the terminal to the TOE. It is based on the Certificate Holder Authorization Template (CHAT). A CHAT is calculated as an AND-operation from the certificate chain of the terminal and the electronic document presenter's restricting input at the terminal. The final CHAT reflects the *effective authorization level* and is then sent to the TOE [TR03110-3]. For the access rights, cf. also the SFR component FDP_ACF.1/TRM in Chapter 6.1.3.

All necessary certificates of the related public key infrastructure – Country Verifying Certification Authority (CVCA) Link Certificates, Document Verifiers Certificates and Terminal Certificates – must be available in the card verifiable format defined in [TR03110-3].

The term *terminal* within this ST usually refers to any kind of terminal, if not explicitly mentioned otherwise . An overview of which of the above terminals are related to what application, and which data group is accessible is provided.

Terminal	ePass	eSign	eID
PACE terminal	Read DG1-DG16 of the ICAO ePass except for DG3 and DG4	-	-
EAC1 terminal[1]	Read ICAO ePass, DG3 and DG4 and optional DG5-DG13	-	-
EAC 2 terminal[2]	Read DG1-DG16 of the ePass (i.e. all data groups)	Access to the digital signature functionality	Read DG1-DG22 of the eID Write DG17-DG22
Update terminal[3]	-	-	-

Table 1 Overview of the user data accessible using the different terminal types

Other terminals than the above are out of scope of this ST. In particular, terminals using Basic Access Control (BAC) are functionally supported by the electronic document, but if the TOE is operated using BAC, it is not in a certified mode.

1.2.7 TOE Design

The electronic document has three different configurations, each being one of the following combinations of applications and protocols:

[1] An EAC1 terminal can access all the data that can be accessed with a PACE terminal.

[2] An EAC2 terminal can access all the data that can be accessed with a PACE terminal.

[3] An update terminal is used to read info about the TOE software or install a new version of the TOE software but has no access to the applications.

- *Passport configuration* (STARCOS 3.7 ID ePA C1): user data stored in an ICAO-compliant ePass application protected by PACE and EAC1. Here, EAC1 is used only for data groups 3 and 4.

- *Residence permit configuration* (STARCOS 3.7 ID ePass C1): user data stored in an ICAO-compliant ePass application protected by PACE and EAC1/EAC2. Additional user data are stored in [TR03110-2] conformant eID and eSign applications, and are protected by EAC2 (STARCOS 3.7 ID eAT C1).

- *Electronic Document configuration* (STARCOS 3.7 ID ePass C1): user data contained in [TR03110-2]-conformant eID, and eSign applications. An ePass application is included as well, but not compliant to [ICAO9303], since user data of all applications are protected by PACE/EAC2.

The purpose and usage of the above mentioned different applications is as follows:

- An **ePass application**, as defined in [ICAO9303], is intended to be used by authorities as a machine readable travel document (MRTD). For the ePassport application, the electronic document holder can control access to his user data by consciously presenting his electronic document to authorities[4].
- An **eID application**, as defined in [TR03110-2], including related user data and data needed for authentication, is intended to be used for accessing official and commercial services which require access to user data stored in the application. For an eID application, the electronic document holder can control access to his user data by inputting his secret PIN (eID-PIN) or by consciously presenting his electronic document to authorities[5];
- An **eSign application**, as defined in [TR03110-2], is intended to generate qualified electronic signatures. The main specific property distinguishing qualified electronic signatures from other, i.e. advanced electronic signatures, is that they are based on qualified certificates and created by secure signature creation devices (SSCD). An eSign application, if implemented, can optionally be activated on the electronic document by a Certification Service Provider, or on his behalf. For an eSign application, the electronic document holder can control access to the digital signature functionality by consciously presenting his electronic document to an EAC2 terminal and inputting his secret PIN (eSign-PIN) for this application[6].

Each application contains its own set of user data, composed according to its requirements.

Application note 5: While it is technically possible to grant access to the electronic signature functionality by inputting only the CAN (see

[4] CAN or MRZ user authentication, see [TR03110-1]

[5] eID-PIN or CAN user authentication, see [TR03110-2]

[6] 3CAN and eSign-PIN user authentication, see [TR03110-2]

[TR03110-2]), this technical option is not be allowed by the security policy defined for the eSign application; see the related conformance claim in section 2.2. This is due to the fact that solely the signatory – which is here the electronic document holder – is able to generate an electronic signature on his own behalf.

Application note 6: Requiring the document holder to use a separate eSign-PIN to generate qualified signatures represents a manifestation of his declaration of intent bound to this secret PIN. The eID and the eSign applications are provided with organizationally different values of the respective secret PINs (eID-PIN and eSign-PIN).

1.2.8 Configurations of the TOE

The TOE can be used in three different configurations:

1. STARCOS 3.7 ID ePA C1 configuration, corresponding to the “electronic Document configuration” described in [MR.ED2.0].
2. STARCOS 3.7 ID eAT C1 configuration, corresponding to the “Residence permit configuration” described in [MR.ED2.0].
3. STARCOS 3.7 ID ePass C1 configuration, corresponding to the “Passport configuration” described in [MR.ED2.0].

In life cycle phase 2 and 3 the specific TOE configuration can be identified by the TOE response to a specific APDU specified in the TOE documentation (see chapter 1.1).

1.2.9 Physical Scope of TOE

The TOE consists of the following parts:

- The hardware platform Infineon IFX_CCI_000005h (Certificate: BSI-DSZ-CC-1110-V3-2020), with the following configurations according to [HWST]
  - FLASH
  - ROM (not available)
  - RAM
  - SCP (Symmetric Crypto Co-processor for DES and AES Standards): accessible
  - Crypto2304T (Crypto Co-processor for asymmetric algorithms like RSA and EC): accessible
  - Interfaces: ISO/IEC 7816 and/or ISO/IEC 14443
- STARCOS 3.7 operation system

- ePA, eAT or ePass applications (the dedicated files for the ePassport, the eID-and the eSign application in a file system, see 1.2.8 for the different configurations of the TOE).

1.2.10 Logical Scope of the TOE

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

- only authenticated terminals can get access to the user data stored on the TOE and use security functionality of the electronic document according to the access rights of the terminal,
- the electronic document holder can control access by entering his secret PIN,
- authenticity and integrity of user data can be verified,
- confidentiality of user data in the communication channel between the TOE and the connected terminal is provided,
- inconspicuous tracing of the electronic document is averted,
- its security functionality and the data stored inside are self-protected, and
- digital signatures can be created, in the configurations of the TOE containing an eSign application.

It allows to update the TOE software during the life-cycle phase *operational use.*

2 Conformance Claim

2.1 CC Conformance Claim

This security target 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, Apr 2017 [CC1]

Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, Apr 2017 [CC2]

Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, Apr 2017 [CC3]

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, Apr 2017, [CC4]

has to be taken into account.

2.2 PP Claim

This ST claims strict conformance to the Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED2.0], ver. 2.0.3, 18.07.2016, BSI-CC-PP-0087-V2-MA-01.

Furthermore, this ST claims strict conformance with the Machine-Readable Electronic Documents –Optionales Nachladen (Optional Post-Emission Updates) [MR.ED-ON-PP], in a configuration with [MR.ED2.0] as the single base PP.

2.3 Package Claim

The current ST is conformant to the following security requirements package:

Assurance package EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 as defined in the CC, part 3 [CC3].

2.4 Conformance Claim Rationale

This ST conforms to the PPs [EAC1PP], [EAC2PP] and [SSCDPP].This implies for this ST:

- The TOE type of this ST is the same[7] as the TOE type of the claimed PPs: The Target of Evaluation (TOE) is an electronic document implemented as a smart card programmed according to [TR03110-1] and [TR03110-2], and for the eSign application additionally representing a combination of hardware and software configured to securely create, use and manage signature-creation data.
- The security problem definition (SPD) of this ST contains the SPD of the claimed PPs. The SPD contains all threats, organizational security policies and assumptions of the claimed PPs and identifies additional threats T.InconsistentSec and T.Interfere.
- The security objectives for the TOE in this ST include all the security objectives for the TOE of the claimed PPs, and add the security objective OT.Non_Interfere. This objective does not weaken the security objectives of the claimed PPs.
- The security objectives for the operational environment in this ST include all security objectives for the operational environment of the claimed PPs.
- The SFRs specified in this ST include all security functional requirements (SFRs) specified in the claimed PPs. We especially point to the following three refined SFRs within this ST:The SFR **FIA_UAU.1/SSCDPP** is redefined from [SSCDPP] by additional assignments. Note that this does not violate strict conformance to [SSCDPP].Multiple iterations of FDP_ACF.1 and FMT_SMR.1 exist from imported PPs to define the access control SFPs and security roles for (common) user data, EAC1-protected user data, and EAC2-protected user data. These access control SFPs and security roles are unified to **FDP_ACF.1/TRM** and **FMT_SMR.1**.
- The SARs specified in this ST are the same as specified in the claimed PPs or extend them.

[7] see also the justification in Chapter 1.2.3.

3 Security Problem Definition

3.1 Introduction

3.1.1 Assets

3.1.1.1 **Primary Assets**

As long as they are in the scope of the TOE, the primary assets to be protected by the TOE are listed below. For a definition of terms used, but not defined here, see the Glossary.

Authenticity of the Electronic Document's Chip
The authenticity of the electronic document's chip personalized by the issuing state or organization for the electronic document holder, is used by the electronic document presenter to prove his possession of a genuine electronic document.

Generic Security Property: Authenticity

This asset is equal to the one(s) of [EAC1PP] and [EAC2PP], which itself stem from [PACEPP].

Electronic Document Tracing Data
Technical information about the current and previous locations of the electronic document gathered unnoticeable by the electronic document holder recognizing the TOE not knowing any PACE password. TOE tracing data can be provided / gathered.

Generic Security Property: Unavailability

This asset is equal to the one(s) of [EAC1PP] and [EAC2PP], which itself stem from [PACEPP]. Note that unavailability here is required for anonymity of the electronic document holder.

Sensitive User Data
User data, which have been classified as sensitive data by the electronic document issuer, e. g. sensitive biometric data. Sensitive user data are a subset of all user data, and are protected by EAC1, EAC2, or both.

Generic Security Properties: Confidentiality, Integrity, Authenticity

User Data stored on the TOE
All data, with the exception of authentication data, that are stored in the context of the application(s) on the electronic document. These data are allowed to be *read out, used or modified* either by a PACE terminal, or,

in the case of sensitive data, by an EAC1 terminal or an EAC2 terminal with appropriate authorization level.

Generic Security Properties: Confidentiality, Integrity, Authenticity

This asset is included from [EAC1PP], [EAC2PP] respectively. In these protection profiles it is an extension of the asset defined in [PACEPP]. This asset also includes ”SVD” (Integrity and Authenticity only), “SCD” of [SSCDPP].

User Data transferred between the TOE and the Terminal
All data, with the exception of authentication data, that are transferred (both directions) during usage of the application(s) of the electronic document between the TOE and authenticated terminals.

Generic Security Properties: Confidentiality, Integrity, Authenticity

This asset is included from [EAC1PP], [EAC2PP] respectively. In these protection profiles it is an extension of the asset defined in [PACEPP]. As for confidentiality, note that even though not each data element being transferred represents a secret, [TR03110-1], [TR03110-2] resp. require confidentiality of all transferred data by secure messaging in encrypt-then-authenticate mode. This asset also includes “DTBS” of [SSCDPP].

3.1.1.2 Secondary Assets

In order to achieve a sufficient protection of the primary assets listed above, the following secondary assets also have to be protected by the TOE.

Accessibility to the TOE Functions and Data only for Authorized Subjects
Property of the TOE to restrict access to TSF and TSF-Data stored in the TOE to authorized subjects only.
Generic Security Property: Availability

Genuineness of the TOE
Property of the TOE to be authentic in order to provide claimed security functionality in a proper way.
Generic Security Property: Availability

Electronic Document Communication Establishment Authorization Data
Restricted-revealable authorization information for a human user being used for verification of the authorization attempts as an authorized user (PACE password). These data are stored in the TOE, and are not send to it.
Restricted-revealable here refers to the fact that if necessary, the electronic document holder may reveal her verification values of CAN

and MRZ to an authorized person, or to a device that acts according to respective regulations and is considered trustworthy.
Generic Security Properties: Confidentiality, Integrity

Secret Electronic Document Holder Authentication Data
Secret authentication information for the electronic document holder being used for verification of the authentication attempts as authorized electronic document holder (PACE passwords).
Generic Security Properties: Confidentiality, Integrity

TOE internal Non-Secret Cryptographic Material
Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material used by the TOE in order to enforce its security functionality.
Generic Security Properties: Integrity, Authenticity

TOE internal Secret Cryptographic Keys
Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.
Generic Security Properties: Confidentiality, Integrity

Application Note 7: The above secondary assets represent TSF and TSF-Data in the sense of CC.

In addition to the secondary assets of [MR.ED2.0], the following assets are added:

Secret Cryptographic Update Keys

All cryptographic key material related to the update mechanism; i.e. cryptographic material that is used to establish a secure communication channel with the update terminal, to authenticate an update terminal, to decrypt and verify the authenticity of an update package, and for other update-related cryptographic operations. Note that this term deliberately includes public (in the cryptographic sense) signing keys installed on the TOE for verifying the authenticity of update packages, as well as ephemeral keys.

Meta-Data

Data that contains information about the update, e.g. version information, checksums, information w.r.t. applicability to specific product versions and platforms, etc. The meta-data contained in the TOE are :

- Hardware manufacturer
- Hardware-ID
- Software developer
- Type of card
- Version of the COS compatible with the update

- Version of the update

Update Data

Unencrypted data that is used to update the TOE software.

Note that we use the term *update data* to denote the unencrypted data. Encrypted update data, appended with optional additional unencrypted meta-data (i.e. version number, TOE product identifier), and signed, is called an *update package*.

Update Log Data

Log records that store information about previously applied updates and failed update attempts.

Update Package

Encrypted update data, appended with optional unencrypted meta-data, and signed.

Update Package Verification Status

Security attribute indicating whether the supplied update was successfully verified (and where hence its authenticity and integrity can be assumed) or not, and whether an attempt to verify was made or not. Allowed values are NOT VERIFIED, SUCCESSFULLY VERIFIED and VERIFICATION FAILED.

Version Information

Version information uniquely identifying the version of the TOE software currently installed on the TOE.

3.1.2 Subjects

This security target considers the following external entities and subjects:

Attacker
A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the ST, especially to change properties of the assets that have to be maintained. The attacker is assumed to possess at most high attack potential. Note that the attacker might capture any subject role recognized by the TOE.

Country Signing Certification Authority (CSCA)
An organization enforcing the policy of the electronic document issuer, i. e. confirming correctness of user and TSF data that are stored within the electronic document. The CSCA represents the country specific root of the public key infrastructure (PKI) for the electronic document, and creates Document Signer Certificates within this PKI. The CSCA also

issues a self-signed CSCA certificate that has to be distributed to other countries by secure diplomatic means, see [ICAO9303].

Country Verifying Certification Authority (CVCA)
The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing state or organization, i. e. enforcing protection of sensitive user data that are stored in the electronic document. The CVCA represents the country specific root of the PKI of EAC1 terminals, EAC2 terminals respectively, and creates Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed as CVCA Link-Certificates.

Document Signer (DS)
An organization enforcing the policy of the CSCA. A DS signs the Document Security Object that is stored on the electronic document for Passive Authentication. A Document Signer is authorized by the national CSCA that issues Document Signer Certificate, see [ICAO9303]. Note that this role is usually delegated to a Personalization Agent.

Document Verifier (DV)
An organization issuing terminal certificates as a Certificate Authority, authorized by the corresponding CVCA to issue certificates for EAC1 terminals, EAC2 terminals respectively, see [TR03110-3].

Electronic Document Holder
A person the electronic document issuer has personalized the electronic document for. Personalization here refers to associating a person uniquely with a specific electronic electronic document. This subject includes “Signatory” as defined [SSCDPP].

Electronic Document Presenter
A person presenting the electronic document to a terminal and claiming the identity of the electronic document holder. Note that an electronic document presenter can also be an attacker. Moreover, this subject includes “User” as defined in [SSCDPP].

Manufacturer
Generic term comprising both the IC manufacturer that produces the integrated circuit, and the electronic document manufacturer that creates the electronic document and attaches the IC to it. The manufacturer is the default user of the TOE during the manufacturing life cycle phase. When referring to the role manufacturer, the TOE itself does not distinguish between the IC manufacturer and the electronic document manufacturer.

PACE Terminal
A technical system verifying correspondence between the password stored in the electronic document and the related value presented to the terminal by the electronic document presenter. A PACE terminal implements the terminal part of the PACE protocol and authenticates

itself to the electronic document using a shared password (CAN, eID-PIN, eID-PUK or MRZ). A PACE terminal is not allowed reading sensitive user data.

Personalization Agent
An organization acting on behalf of the electronic document issuer that personalizes the electronic document for the electronic document holder. Personalization includes some or all of the following activities: (i) establishing the identity of the electronic document holder for the biographic data in the electronic document, (ii) enrolling the biometric reference data of the electronic document holder, (iii) writing a subset of these data on the physical electronic document (optical personalization) and storing them within the electronic document's chip (electronic personalization), (iv) writing document meta data (i. e. document type, issuing country, expiry date, etc.) (v) writing the initial TSF data, and (vi) signing the Document Security Object, and the elementary files EF.CardSecurity and the EF.ChipSecurity (if applicable [ICAO9303], [TR03110-3]) in the role DS. Note that the role personalization agent may be distributed among several institutions according to the operational policy of the electronic document issuer. This subject includes “Administrator” as defined in [SSCDPP].

EAC1 Terminal / EAC2 Terminal
A terminal that has successfully passed the Terminal Authentication protocol (TA) version 1 is an EAC1 terminal, while an EAC2 terminal needs to have successfully passed TA version 2. Both are authorized by the electronic document issuer through the Document Verifier of the receiving branch (by issuing terminal certificates) to access a subset or all of the data stored on the electronic document.

Terminal
A terminal is any technical system communicating with the TOE through the contactless or contact-based interface. The role *terminal* is the default role for any terminal being recognized by the TOE as neither being authenticated as a PACE terminal nor an EAC1 terminal nor an EAC2 terminal.

In addition to the subject of [MR.ED2.0], the following subject is added here:

Update Terminal

A terminal to read out version information and update log data of the TOE software, and to install updates of the TOE software. Prior executing these functions, the update terminal must authenticate itself towards the TOE.

3.2 Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats

result from the assets protected by the TOE and the method of the TOE's use in the operational environment.

T.InconsistentSec **Inconsistency of security measures**

Adverse action: An attacker gains read or write access to user data or TOE data without being allowed to, due to an ambiguous/unintended configuration of the TOE's internal access conditions of user or TSF data. This may lead to a forged electronic document or misuse of user data.

Threat agent: having high attack potential, being in possession of one or more legitimate electronic documents

Asset: authenticity, integrity and confidentiality of user data stored on the TOE

T.Interfere **Interference of security protocols**

Adverse action: An attacker uses an unintended interference of implemented security protocols to gain access to user data.

Threat agent: having high attack potential, being in possession of one or more legitimate electronic documents

Asset: authenticity, integrity and confidentiality of user data stored on the TOE

T.AdvancedTracing Compromise **Advanced Tracing and Group Key**

Adverse action: The attacker compromises a group key or is able to trace and dentify the electronic document holder by key material that is used to guarantee the authenticity of the document.

Tracing is often (e.g. in the case of Chip Authentication 2) avoided by using one key for a group of electronic documents. If the group is large enough, individual tracing is no longer possible. If an attacker compromises such a group key however, authenticity of *all* of the electronic documents within the group can be guaranteed. On the other hand, if chip individual keys are used to ensure the authenticity of the document, only a single document is affected by a key compromise. However then, the (public) chip-individual keys can be misused for tracing the document and its holder.

Threat agent: having high attack potential, being in the possession of one or more legitimate electronic documents

Asset: authenticity, integrity, and confidentiality of user data stored on the TOE

3.2.1 Threats from [EAC1PP]

This ST includes the following threats from [EAC1PP]. They concern EAC1-protected data.

- **T.Counterfeit**
- **T.Read_Sensitive_Data**

Due to identical definitions and names they are not repeated here. For the remaining threats from [EAC1PP], cf. Chapter 3.2.3.

3.2.2 Threats from [EAC2PP]

This ST includes the following threats from the [EAC2PP]. They concern EAC2-protected data.

- **T.Counterfeit/EAC2**
- **T.Sensitive_Data**

Due to identical definitions and names, they are not repeated here.

3.2.3 Threats from [PACEPP]

Both [EAC1PP] and [EAC2PP] claim [PACEPP], and thus include the threats formulated in [PACEPP]. We list each threat only once here. Due to identical definitions and names, their definitions are not repeated here.

- **T.Abuse-Func**
- **T.Eavesdropping**
- **T.Forgery**
- **T.Information_Leakage**
- **T.Malfunction**
- **T.Phys-Tamper**
- **T.Skimming**
- **T.Tracing**

3.2.4 Threats from [SSCDPP]

This ST also includes all threats of [SSCDPP]. These items are applicable if the eSign application is operational.

- **T.DTBS_Forgery**
- **T.Hack_Phys**
- **T.SCD_Derive**
- **T.SCD_Divulge**
- **T.Sig_Forgery**
- **T.SigF_Misuse**

- **T.SVD_Forgery**

Due to identical definitions and names, their definitions are not repeated here.

3.2.5 Threats from [MR.ED-ON-PP]

T.FaTSF Faulty TSF

Adverse action: An attacker gains read or write access to user data or TSF data, or manipulates or mitigates the TSF, for example due to:

- software issues that were not detected, not exploitable, or deemed unable to being exploitable at the time of certification, but due to unforeseen advances in technology became a security risk during operational use of the TOE, or
- cryptographic mechanisms that were deemed secure at the time of certification, but due to unforeseen advances in the field of cryptography became a security risk during operational use of the TOE.

Threat agent: having high attack potential, being in possession of one or more legitimate electronic documents

Asset: all data stored on the TOE (esp. the integrity, authenticity and – if applicable – secrecy of the data)

T.UaU Unauthorized Update

Adverse action: An attacker gains read or write access to user data or TSF data, or manipulates or mitigates the TSF by misuse of the update functionality. This threat contains two main aspects:

- the unauthorized installation, which may lead to the use of untimely, outdated or revoked updates.
- the installation of updates that are not authorized and authentic.

Threat agent: having high attack potential, being in possession of one or more legitimate electronic documents

Asset: all data stored on the TOE (esp. the integrity, authenticity and – if applicable – secrecy of the data)

3.3 Organisational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC1, sec. 3.2). This ST includes the OSPs from the claimed protection profiles as listed below and provides no further OSPs.

3.3.1 OSPs from [EAC1PP]

This ST includes the following OSPs from [EAC1PP], for the configurations of the TOE containing EAC1-protected data.

- **P.Personalisation**
- **P.Sensitive_Data**

Due to identical definitions and names, they are not repeated here. For the remaining OSPs from [EAC1PP], see the next sections.

3.3.2 OSPs from [EAC2PP]

This ST includes the following OSPs from [EAC2PP]. They mainly concern EAC2-protected data.

- **P.EAC2_Terminal**
- **P.RestrictedIdentity**
- **P.Terminal_PKI**

Due to identical definitions and names, their definitions are not repeated here. For the remaining OSPs from [EAC2PP], cf. the next section.

3.3.3 OSPs from [PACEPP]

This ST includes the following OSPs from [PACEPP], since both [EAC1PP] and [EAC2PP] claim [PACEPP]. We list each OSP only once here. Due to identical definitions and names, their definitions are not repeated here as well.

- **P.Card_PKI**
- **P.Manufact**
- **P.Pre-Operational**
- **P.Terminal**
- **P.Trustworthy_PKI**

3.3.4 OSPs from [SSCDPP]

This ST also includes all OSPs of [SSCDPP]. They are applicable, if the eSign application is included.

- **P.CSP_QCert**
- **P.QSign**
- **P.Sig_Non-Repud**
- **P.Sigy_SSCD**

Due to identical definitions and names, their definitions are not repeated here.

3.3.5 OSPs from [MR.ED-ON-PP]

P.Code_Confidentiality

Update code packages that are created by the TOE software developer or document manufacturer are kept confidential, are encrypted after development at the site of the electronic document manufacturer, and are delivered to the TOE in encrypted form.

P.Secure_Environment

Update terminals are placed in a secure environment that prevents unauthorized physical access, and are operated by authorized staff only. Authorized staff oversees the complete update procedure.

P.Eligible_Terminals_Only

Update terminals (i.e. terminals with appropriate certificates that are able to install updates) are handed only to those entities where P.Secure_Environment is enforced. In case of a security incident, these update terminals are functionally disabled (through organizational and/or cryptographic means by e.g. withdrawing certificates).

3.3.6 Additional OSPs

The next OSP addresses the need of a policy for the document manufacturer. It is formulated akin to [ICPP].

P.Lim_Block_Loader

The composite manufacturer uses the Loader for loading of Security IC Embedded Software, user data of the Composite Product or IC Dedicated Support Software in charge of the IC Manufacturer. She limits the capability and blocks the availability of the Loader in order to protect stored data from disclosure and manipulation.

3.4 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used. This ST includes the assumptions from the claimed protection profiles as listed below and defines no further assumptions.

3.4.1 Assumptions from [EAC1PP]

This ST includes the following assumptions from the [EAC1PP]. They concern EAC1-protected data.

- **Auth_PKI**
- **Insp_Sys**

Due to identical definitions and names, their definitions are not repeated here. For the remaining assumptions from [EAC1PP], see the next sections.

3.4.2 Assumptions from [EAC2PP]

[EAC2PP] only includes the assumption from [PACEPP] (see below) and defines no other assumption.

3.4.3 Assumptions from [PACEPP]

This ST includes the following assumptions from [PACEPP], since both [EAC1PP] and [EAC2PP] claim [PACEPP].

- **A.Passive_Auth**

Due to an identical definition and name, its definition is not repeated here as well.

3.4.4 Assumptions from [SSCDPP]

This ST also includes all assumptions of [SSCDPP]. These items are applicable, if the eSign application is included.

- **A.CGA**
- **A.SCA**

4 Security Objectives

This chapter describes the security objectives for the TOE and for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development, and production environment and security objectives for the operational environment.

4.1 Security Objectives for the TOE

This section describes the security objectives for the TOE, addressing the aspects of identified threats to be countered by the TOE, and organizational security policies to be met by the TOE.

OT.Non_Interfere No interference of Access Control Mechanisms

The various implemented access control mechanisms must be consistent. Their implementation must not allow to circumvent an access control mechanism by exploiting an unintended implementational interference of one access control mechanism with another one.

4.1.1 Security Objectives for the TOE from [EAC1PP]

This ST includes the following additional security objectives for the TOE from [EAC1PP] that are not included in [PACEPP]. They concern EAC1-protected data.

- **OT.Chip_Auth_Proof**
- **OT.Sens_Data_Conf**

Due to identical definitions and names, their definitions are not repeated here. For the remaining security objectives from [EAC1PP], see the next sections.

In addition, the following security objective is defined here:

OT.Chip_Auth_Proof_PACE_CAM Proof of the electronic document's chip authenticity
The TOE must support the terminals to verify the identity and authenticity of the electronic document's chip as issued by the identified issuing State or Organization by means of the PACE-Chip Authentication Mapping (PACE-CAM) as defined in [ICAO9303]. The authenticity proof provided by electronic document's chip shall be protected against attacks with high attack potential.

Application note 8: PACE-CAM enables much faster authentication of the chip than running PACE with Generic Mapping (according to [TR03110-1]) followed by CA1. OT.Chip_Auth_Proof_PACE_CAM is intended to require the Chip to merely provide an additional means – with the same level of security – of authentication.

4.1.2 Security Objectives for the TOE from [EAC2PP]

This ST includes the following additional security objectives for the TOE from [EAC2PP] that are not included in [PACEPP]. They concern EAC2-protected data.

- **OT.AC_Pers_EAC2**
- **OT.CA2**
- **OT.RI_EAC2**
- **OT.Sens_Data_EAC2**

Due to identical definitions and names, their definitions are not repeated here. In addition, the next security objective is added:

OT.CA3 Protection against advanced tracing techniques using Chip Authentication 3
The TOE provides the Chip Authentication 3 protocol. Chip Authentication 3 provides a message-deniable strong explicit authentication of the electronic document, pseudonymity of the electronic document without the need to use the same keys on several chips, and the possibility of whitelisting electronic documents, even in the case of a group key compromise. (cf. [TR03110-2-v2.20]).

4.1.3 Security Objectives for the TOE from [PACEPP]

Both [EAC1PP] and [EAC2PP] claim [PACEPP]. Therefore the following security objectives are included as well. We list them only once here.

- **OT.AC_Pers**
- **OT.Data_Authenticity**
- **OT.Data_Confidentiality**
- **OT.Data_Integrity**
- **OT.Identification**
- **OT.Prot_Abuse-Func**
- **OT.Prot_Inf_Leak**
- **OT.Prot_Malfunction**
- **OT.Prot_Phys-Tamper**
- **OT.Tracing**

Due to identical definitions and names, their definitions are not repeated here.

4.1.4 Security objectives for the TOE from [SSCDPP]

This ST also includes all security objectives for the TOE of [SSCDPP]. These items are applicable, if an eSign application is included.

- **OT.DTBS_Integrity_TOE**
- **OT.EMSEC_Design**
- **OT.Lifecycle_Security**
- **OT.SCD_Secrecy**
- **OT.SCD_SVD_Corresp**
- **OT.SCD_Unique**
- **OT.SCD/SVD_Auth_Gen**

- **OT.Sig_Secure**
- **OT.Sigy_SigF**
- **OT.Tamper_ID**
- **OT.Tamper_Resistance**

Due to identical definitions and names, their definitions are not repeated here as well. Note that all are formally included here, but careful analysis reveals that OT.SCD_Secrecy, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID, and OT.Tamper_Resistance are actually fully or partly covered by security objectives included from [PACEPP].

4.1.5 Security Objectives for the TOE from [MR.ED-ON-PP]

OT.Update_Mechanism **TOE Update Mechanism**

The TSF provides a mechanism to install code-signed updates of the TOE software by authorized staff during operational use.

OT.Enc_Sign_Update Packages **Encrypted-then-signed Update**

The TOE only installs update packages that are encrypted, integrity-protected and signed by the authority in charge of delivering and installing updates.

OT.Update_Terminal_Auth **Updates only by authenticated Update Terminals**

The TOE allows only authenticated update terminals to upload an update package to the TOE and to initiate the update procedure. The TOE uses a dedicated cryptographic method (to be defined or referenced by the ST-Writer) to authenticate an update terminal.

OT.Attack_Detection using the Update Mechanism **Detection of Attacks on the TOE**

The TOE has logging capabilities that track installed updates and failed update attempts. It also limits the amount of faulty (signature verification or decryption fails) update attempts. It allows dedicated terminals to read out the update logs.

OT.Key_Secrecy **Key Secrecy of Cryptographic Update Keys**

The TOE keeps the cryptographic update keys secret, and is designed such that emissions from the TOE do not allow to read out or gain full or partial information about the keys.

4.1.6 Additional Security Ojectives for the TOE

A loader is a part of the chip operating system that allows to load data, i.e. the file-system/applet containing (sensitive) user data, TSF data etc. into the Flash or EEPROM memory after delivery of the smartcard to the document manufacturer.

The following objective for the TOE addresses limiting the availability of the loader, and is formulated akin to [ICPP].

OT.Cap_Avail_Loader
The TSF provides limited capability of the Loader functionality of the TOE embedded software and irreversible termination of the Loader in order to protect user data from disclosure and manipulation.

4.2 Security Objective for the Development and Production Environment

[MR.ED-ON-PP] defines a security objective for the Development and Production Environment:

OE.Code_Confidentiality

The operational environment must ensure that the TOE software developer or document manufacturer keeps update code packages confidential, encrypts them after development at the site of the developer/manufacturer, and delivers them to the TOE in encrypted form.

4.3 Security Objectives for the Operational Environment

4.3.1 Security objectives from [EAC1PP]

This ST includes the following security objectives for the TOE from the [EAC1PP]. They mainly concern EAC1-protected data.

- **OE.Auth_Key_Travel_Document**
- **OE.Authoriz_Sens_Data**
- **OE.Exam_Travel_Document**
- **OE.Ext_Insp_Systems**
- **OE.Prot_Logical_Travel_Document**

Due to identical definitions and names, their definitions are not repeated here. For the remaining ones, see the next sections.

4.3.2 Security Objectives from [EAC2PP]

This ST includes the following security objectives for the TOE from the [EAC2PP]. They mainly concern EAC2-protected data.

- **OE.Chip_Auth_Key**
- **OE.RestrictedIdentity**
- **OE.Terminal_Authentication**

Due to identical definitions and names, their definitions are not repeated here. For the remaining ones, see the next section.

4.3.3 Security Objectives from [PACEPP]

Both [EAC1PP] and [EAC2PP] claim [PACEPP]. Therefore the following security objectives on the operational environment are included as well. We repeat them only once here.

- **OE.Legislative_Compliance**
- **OE.Passive_Auth_Sign**
- **OE.Personalisation**
- **OE.Terminal**
- **OE.Travel_Document_Holder**

Due to identical definitions and names, they are not repeated here as well.

4.3.4 Security Objectives from [SSCDPP]

This ST also includes all security objectives for the TOE of [SSCDPP]. These items are applicable, if an eSign application is included.

- **OE.CGA_QCert**
- **OE.DTBS_Intend**
- **OE.DTBS_Protect**
- **OE.HID_VAD**
- **OE.Signatory**
- **OE.SSCD_Prov_Service**
- **OE.SVD_Auth**

Due to identical definitions and names, their definitions are not repeated here.

4.3.5 Security Objectives from [MR.ED-ON-PP]

OE.Secure_Environment

The operational environment must ensure that update terminals are placed in a secure environment that prevents unauthorized physical access, and are operated by authorized staff only. The operational environment must also ensure through e.g. organizational policies and

procedures, that authorized staff oversees the complete update procedure.

OE.Eligible_Terminals_Only

The operational environment must also ensure by e.g. organizational procedures, supported by cryptographic means, that only those entities that have policies in place that guarantee OE.Secure_Environment, are supplied with update terminals. Moreover the operational environment guarantees that update terminals can be functionally deactivated if these policies are no longer in place or not enforced at the entities. This can be implemented for example by the issuance of certificates for update terminals together with a public key infrastructure.

Justification: Each of these security objectives on the environment directly addresses one of the organizational security policies P.Code_Confidentiality, P.Secure_Environment, and P.Eligible_Terminals_Only. Hence, these security objectives for the environment do

- neither mitigate a threat of the base PP that was addressed by security objectives of the base PP,
- nor do they fulfill any organizational security policy of the base PP that was meant to be addressed by security objectives of the TOE of the base PP.

Note in particular that OE.Eligible_Terminals_Only requires a general issuance and revocation mechanism for update terminals and leaves the specific implementation open, whereas OE.Terminal_Authentication of the base PP specifically addresses certificates for EAC2 terminals.

4.3.6 Additional Security Objectives for the Environment

The following objective on the environment is defined akin to the objective from [ICPP].

OE.Lim_Block_Loader
The manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.

Justification: This security objective directly addresses the threat **OT.Non_Interfere**. This threat concerns the potential interference of different access control mechanisms, which could occur as a result of combining different applications on a smartcard. Such combination does not occur in one of the claimed PPs. Hence, this security objective for the environment does

- neither mitigate a threat of one of the claimed PPs that was addressed by security objectives of that PP,

- nor does it fulfill any organizational security policy of one of the claimed PPs that was meant to be addressed by security objectives of the TOE of that PP.

4.4 Security Objective Rationale

Table 2 provides an overview of the security objectives' coverage. According to [CC1], the tracing between security objectives and the security problem definition must ensure that 1) *each security objective traces to at least one threat, OSP and assumption*, 2) *each threat, OSP and assumption has at least one security objective tracing to it*, and 3) *the tracing is correct* (i.e. the main point being that security objectives for the TOE do not trace back to assumptions).

This is illustrated in the following way:

1) can be inferred for security objectives from claimed PPs by looking up the security objective rationale of the claimed PPs and for newly introduced security objectives (i.e. **OE.Lim_Block_Loader** and **OT.Cap_Avail_Loader, OT.CA3 and OT.Chip_Auth_Proof_PACE_CAM**) by checking the *columns* of Table 2,
2) can be inferred for threats, OSPs and assumptions from the claimed PPs by looking up the security objective rationale of the claimed PPs and for newly introduced threats, OSPs and assumptions by checking the rows of Table 2, and
3) simply by checking the *columns* of Table 2 and the security objective rationales from the claimed PPs.

	OT.AC_Pers	OT.AC_Pers_EAC2	OT.Cap_Avail_Loader	OT.Chip_Auth_Proof_PACE_CAM	OT.CA3	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Non_Interfere	OT.Sens_Data_Conf (EAC1PP)	OT.Sens_Data_EAC2	OE.Lim_Block_Loader
T.InconsistentSec	x	x	x			x	x	x	x	x	x	x
T.Interfere									x			
T.Counterfeit				x								
T.Counterfeit/EAC2					x							
T.AdvancedTracing					x							
P.Lim_Block_Loader			x						x			x

Table 2 Security Objective Rationale

The threat **T.InconsistentSec** addresses attacks on the confidentiality and the integrity of user data stored on the TOE, facilitated by the data not being protected as intended.
OT.AC_Pers and OT.AC_Pers_EAC2 define the restriction on writing or modifying data; OT.Data_Authenticity, OT.Data_Confidentiality, OT.Data_Integrity, OT.Sens_Data_Conf (from [EAC1PP]), and OT.Sens_Data_EAC2 require the security of stored user data as well as user data that are transferred between the TOE and a terminal to be secure w.r.t. authenticity, integrity and confidentiality.
OT.Non_Interfere requires the TOE's access control mechanisms to be implemented consistently and their implementations not to allow to circumvent an access control mechanism by exploiting an unintended implementational interference of one access control mechanism with another one.
OT.Cap_Avail_Loader requires the TOE to provide limited capability of the loader functionality and irreversible termination of the loader in order to protect stored user data.
OE.Lim_Block_Loader requires the manufacturer to protect the loader functionality against misuse, limit the capability of the loader, and terminate irreversibly the loader after intended usage of the loader.

The combination of these security objectives cover the threat posed by **T.InconsistentSec**.

The threat **T.Interfere** addresses the attack on user data by exploiting the unintended interference of security protocols. This is directly countered by OT.Non_Interfere, requiring the TOE's access control mechanisms to be implemented consistently, and their implementations to not allow to circumvent an access control mechanism by exploiting an unintended implementational interference of one access control mechanism with another one.

The threat **T.Counterfeit** (from [EAC1PP]) is countered in [EAC1PP] by OT.Chip_Auth_Proof. That security objectives addresses the implementation of the Chip Authentication Protocol Version 1 (CA1) and thus counters the thread of counterfeiting an electronic document containing an ePassport application. Here, the additional security objective for the TOE OT.Chip_Auth_Proof_PACE_CAM is introduced. It ensures that the chip in addition to CA1 also supports the PACE-Chip Authentication Mapping (PACE-CAM) protocol, which supports the same security functionality as CA1 does. PACE-CAM enables much faster authentication of the chip than running PACE with general mapping followed by CA1.

The threat **T.Counterfeit/EAC2** (from [EAC2PP]) is here countered with OT.CA3 in addiction to OT.CA2 ([EAC2PP]),, since Chip Authentication 3 provides a superset of functions of Chip Authentication 2.

The threat **T.AdvancedTracing** is countered with OT.CA3. The main feature of Chip Authentication 3 is that cryptographic mechanisms are employed to provide pseudonymity of the electronic document without the need to use the same keys on several chips. This directly counters the described threat.

The OSP **P.Lim_Block_Loader** addresses limiting the capability and blocking the availability of the Loader in order to protect stored data from disclosure and manipulation. This is addressed by OT.Cap_Avail_Loader, which requires the TOE to provide a limited capability of the loader functionality and irreversible termination of the loader in order to protect stored user data; by OT.Non_Interfere, which requires the TOE's access control mechanisms to be implemented consistently and their implementations not to allow to circumvent an access control mechanism by exploiting an unintended implementational interference of one access control mechanism with another one; and by OE.Lim_Block_Loader, which requires the manufacturer to protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.

4.4.1 Security Objective Rationale from [MR.ED-ON-PP]

4.4.1.1 Tracings

Table 3 provides an overview of the security objectives' coverage. According to [CC1], the tracing between security objectives and the security problem definition must ensure that 1) each security objective traces to at least one threat, OSP and assumption, 2) each threat, OSP and assumption has at least one security objective tracing to it, and 3) the tracing is correct (i.e. the main point being that security objectives for the TOE do not trace back to assumptions).

	OT.Update_Mechanism	OT.Enc_Sign_Update	OT.Update_Terminal_Auth	OT.Attack_Detection	OT.Key_Secrecy	OE.Code_Confidentiality	OE.Secure_Environment	OE.Eligible_Terminals_Only
T.FaTSF	x			x	x			
T.UaU		x	x					
P.Code_Confidentiality						x		
P.Secure_Environment							x	
P.Eligible_Terminals_Only								x

Table 3 Security Objective Rationale from [**MR.ED-ON-PP**]

Justifications

The threat T.FaTSF addresses attacks on the TOE and TSF by an attacker exploiting flaws of the TOE software implementation that manifest themselves after the TOE enters the phase operational usage. This threat is countered by the TOE offering a secure update mechanism; in particular:

- The security objective OT.Update_Mechanism counters this threat by ensuring that the TOE has the ability to update the TOE software in a secure manner.
- The security objective OT.Attack_Detection ensures that the TOE is able to detect multiple failed update attempts and can take action upon that detection.
- The security objective OT.Key_Secrecy makes sure that the required cryptographic key material for the update mechanism cannot be accessed or reconstructed by a malicious attacker.

The threat **T.UaU** addresses attacks on the TOE and TSF by an attacker installing unauthorized and potential harmful updates:

- The security objective OT.Enc_Sign_Update ensures that only signed and encrypted updates are installed by the TOE, and that during the transmission to the TOE, a protocol based on encrypt-then-MAC is used.
- The security objective OT.Update_Terminal_Auth ensures that only authenticated update terminals are able to read version information, upload update packages on the TOE, and initiate the update procedure.

The organizational security policies **P.Code_Confidentiality**, **P.Secure_Environment**, and **P.Eligible_Terminals_Only**, address the confidentiality of the code, the way the update procedure must be carried out, and precise control over which terminals are allowed to carry out the update procedure. Each of these policies are enforced through security objectives for the environment of the TOE, namely OE.Code_Confidentiality, OE.Secure_Environment, and OE.Eligible_Terminals_Only.

5 Extended Components Definition

This ST includes all extended components from the claimed PPs. This includes

- FAU_SAS.1 from the family FAU_SAS from [PACEPP]
- FCS_RND.1 from the family FCS_RND from [PACEPP]
- FMT_LIM.1 and FMT_LIM.2 from the family FMT_LIM from [PACEPP]
- FPT_EMS.1 from the family FPT_EMS from [PACEPP]
- FIA_API.1 from the family FIA_API from [EAC2PP]

For precise definitions we refer to [PACEPP] and [EAC2PP].

6 Security Requirements

This part defines detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the *functional* and *assurance* security requirements that the TOE must satisfy in order to meet the security objectives for the TOE.

Common Criteria allows several operations to be performed on security requirements on the component level: *refinement*, *selection*, *assignment* and *iteration,* cf. sec. 8.1 of [CC1]. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed words are ~~crossed out.~~

The **selection** operation is used to select one or more options provided by CC in stating a requirement. Selections that have been made by the PP author are denoted as underlined text. Selections filled in by the ST author are denoted as double underlined text and a foot note where the selection choices from the PP are listed.

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 PP author are denoted as underlined text. Assignments filled in by the ST author are denoted as double underlined text.

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. For the sake of better readability, the iteration operation may also be applied to a non-repeated single component in order to indicate that such component belongs to a certain functional cluster. In such a case, the iteration operation is applied to only one single component.

In order to distinguish between SFRs defined here and SFRs that are taken over from PPs to which this ST claims strict conformance, the latter are iterated resp. renamed in the following way:
/EAC1PP or /XXX_EAC1PP [EAC1PP],
/EAC2PP or /XXX_EAC2PP for [EAC2PP],
/SSCDPP or /XXX_SSCDPP for [SSCDPP],
and /MREDONPP or /XXX_MREDONPP for [MR.ED-ON-PP].

6.1 Security Functional Requirements

The statements of security requirements must be internally consistent. As several different PPs with similar SFRs are claimed, great care must be taken to ensure that these several iterated SFRs do not lead to inconsistency.
Both [EAC1PP] and [EAC2PP] claim strict conformance to [PACEPP]. Thus they include all SFRs from [PACEPP]. On the other hand, due to strict conformance to [EAC1PP] and [EAC2PP], [MR.ED2.0] includes all SFRs from [EAC1PP] and [EAC2PP]. **Hence all SFRs from [**PACEPP**] appear in this ST twice as SFRs from [**EAC1PP**] and [**EAC2PP**], and thus SFRs from [**PACEPP**] are not listed in this ST. In other words, despite claiming strict conformance to [**PACEPP**], SFRs can be safely ignored during evaluation and certification as long as [**EAC1PP**] and [**EAC2PP**] are taken into account.**

One must remember that each of these iterated SFRs mostly concerns different (groups of) user and TSF data for each protocol (i.e. PACE, EAC1 and EAC2). We distinguish three cases:

1. The SFRs apply to different data that are accessible by executing different protocols. Hence, they are completely separate. An example is FCS_CKM.1/DH_PACE from [EAC1PP] and [EAC2PP]. No remark is added in such case in the text below.
2. The SFRs are equivalent. Then we list them all for the sake of completeness. Hence, it suffices to consider only one iteration. For such SFRs, we explicitly give a remark. An example is FIA_AFL.1/PACE from [EAC1PP] and [EAC2PP].
3. The SFRs do not apply to different data or protocols, but are also not completely equivalent. Then these multiple SFRs are refined in such a way, that one common component is reached that subsumes all iterations that stem from the inclusions of the claimed PPs. An example is FDP_ACF.1, which is combined here from [EAC1PP] and [EAC2PP]. Such a case is also explicitly mentioned in the text.

Thus internal consistency is not violated.
Last, we remark that compared to [EAC2PP] the following references in SFRs have been updated:

- The reference [ICAO9303] was updated from the sixth to the seventh edition.
- The document *Technical Report: Supplemental Access Control for Machine Readable Travel Documents, Version - 1.1, 15. April 2014.* was replaced with [ICAO9303], since that technical report has been included in the seventh edition of [ICAO9303].

Since the content of the specifications has not changed, we do not explicitly mark these (editorial) refinements in the SFRs.

6.1.1 Class FCS

The STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1 Card contains the TOE and uses the following ECC brainpool curves:

- P256r1,
- P320r1,
- P384r1, and
- P512r1

see chapter 1.3.2 [TR3116-2].

The following SFRs are imported due to claiming [EAC2PP]. They concern cryptographic support for applications that contain EAC2-protected data groups.

- **FCS_CKM.1/DH_PACE_EAC2PP**

Hierarchical to: No other components

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] not fulfilled, but **justified:** 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/EAC2PP**

FCS_CKM.1.1/DH_PACE_EAC2PP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH compliant to* [TR03111][8] and specified cryptographic key sizes 256, 320, 384 and 512 bit [9,10] that meet the following: [TR03110-2][11].

- **FCS_COP.1/SHA_EAC2PP**

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] not fulfilled, but **justified:** A hash function does not

[8] [assignment: cryptographic key generation algorithm]

[9] [assignment: cryptographic key sizes]

[10] For length of p

[11] [assignment: list of standards]

use any cryptographic key; hence, neither a respective key import nor key generation can be expected here.

FCS_CKM.4 Cryptographic key destruction not fulfilled, but **justified:** A hash function does not use any cryptographic key; hence, a respective key destruction cannot be expected here.

FCS_COP.1.1/SHA_EAC2PP

The TSF shall perform hashing[12] in accordance with a specified cryptographic algorithm SHA-1 and SHA-256[13] and cryptographic key sizes none[14] that meet the following: [FIPS180-4][15].

Application Note 9: For compressing (hashing) an ephemeral public key for DH (TA2 and CA2), the hash function SHA-1 shall be used ([TR03110-3]). According to [MR.ED2.0], the TOE shall implement as hash functions SHA-1 or SHA-224 or SHA-256 for Terminal Authentication 2, cf. [TR03110-3]. Within the normative Appendix of [TR03110-3] 'Key Derivation Function', it is stated that the hash function SHA-1 shall be used for deriving 128-bit AES keys, whereas SHA-256 shall be used for deriving 192-bit and 256-bit AES keys.

- **FCS_COP.1/SIG_VER_EAC2PP**

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] not fulfilled, but **justified**: The root key PK_{CVCA} (initialization data) used for verifying the DV Certificate is stored in the TOE during its personalization in the card issuing life cycle phase[16]. Since importing the respective certificates (Terminal Certificate, DV Certificate) does not require any special security measures except those required by the current SFR (cf. FMT_MTD.3 below), the current ST does not contain any dedicated requirement like FDP_ITC.2 for the import function.

[12] [assignment: list of cryptographic operations]

[13] [assignment: cryptographic algorithm]

[14] [assignment: cryptographic key sizes]

[15] [assignment: list of standards]

[16] as already mentioned, operational use of the TOE is explicitly in focus of the [MR.ED2.0] PP

FCS_CKM.4 Cryptographic key destruction not fulfilled, but **justified**: Cryptographic keys used for the purpose of the current SFR (PK_{PCD}, PK_{DV}, PK_{CVCA}) are public keys; they do not represent any secret, and hence need not to be destroyed.

FCS_COP.1.1/SIG_VER_EAC2PP

The TSF shall perform digital signature verification[17] in accordance with a specified cryptographic algorithm ECDSA with SHA-256, SHA-384 and SHA-512 [18]and cryptographic key sizes 256, 320, 384 and 512 bit [19][20]that meet the following: [TR03111] and [FIPS180-4][21].

Application Note *10*: This SFR is concerned with Terminal Authentication 2, cf. [TR03110-2].

- **FCS_COP.1/PACE_ENC_EAC2PP**

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_EAC2PP**

FCS_CKM.4 Cryptographic key destruction **fulfilled** by **FCS_CKM.4/EAC2PP**

FCS_COP.1.1/PACE_ENC_EAC2PP

The TSF shall perform secure messaging – encryption and decryption[22] in accordance with a specified cryptographic algorithm AES in CBC mode[23] and cryptographic key sizes 128, 192 and 256 bit[24] that meet the following: **[TR03110-3][25]**.

Application Note 11: Refinement of FCS_COP.1.1/PACE_ENC, since here PACE must adhere to [TR03110-3]. All references (both the one in [PACEPP] and [TR03110-3]) itself reference [ISO7816-4] for secure messaging. [TR03110-3] however further restricts the available choice of

[17] [assignment: *list of cryptographic operations*]
[18] [assignment: *cryptographic algorithm*]
[19][assignment: *cryptographic key sizes*]
[20] For length of p
[21] [assignment: *list of standards*]
[22] [assignment: *list of cryptographic operations*]
[23] [selection: *cryptographic algorithm*]
[24] [selection: 128, 192, 256 bit]
[25] [assignment: *list of standards*]

key-sizes and algorithms. Hence, [TR03110-3] is fully (backward) compatible to the reference given in [PACEPP].

- **FCS_COP.1/PACE_MAC_EAC2PP**

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_EAC2PP
FCS_CKM.4 Cryptographic key destruction **fulfilled** by
FCS_CKM.4/EAC2PP

FCS_COP.1.1/PACE_MAC_EAC2PP

The TSF shall perform secure messaging – message authentication code[26] in accordance with a specified cryptographic algorithm CMAC[27] and cryptographic key sizes 128, 192 and 256 bits[28] that meet the following: [**TR03110-3**][29].

Application Note 12: This SFR removes 3DES and restricts to CMAC compared to the SFR of [PACEPP] by selection. Hence, a minimum key-size of 128 bit is required.
In addition, this ST includes all remaining SFRs of [PACEPP]. For the class FCS, these are the following components:

•**FCS_CKM.4/EAC2PP** The *Application Note* in [PACEPP] concerning this component requires the destruction of PACE session keys after detection of an error in a received command by verification of the MAC. While the definition of FCS_CKM.4 remains unaltered, here this component also requires the destruction of sessions keys after a successful run of Chip Authentication 2. The TOE shall destroy the CA2 session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.
•**FCS_RND.1/EAC2PP** The Application Note in [PACEPP] concerning this component requires the

[26] [assignment: list of cryptographic operations]
[27] [selection: cryptographic algorithm]
[28] [assignment: *cryptographic key sizes*] / [selection: ~~112~~ 128, 192, 256 bit]
[29] [assignment: list of standards]

TOE to generate random numbers (random nonces) for PACE. While the definition of FCS_RND.1 remains unaltered, here this component requires the TOE to generate random numbers (random nonce) for all authentication protocols (i.e. PACE, CA2), as required by FIA_UAU.4.

- **FCS_CKM.4/EAC2PP**

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_EAC2PP, **FCS_CKM.1/CA3**

FCS_CKM.4.1/EAC2PP The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the key value with zero values[30] that meets the following: none[31].

- **FCS_RND.1/EAC2PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FCS_RND.1.1/EAC2PP

The TSF shall provide a mechanism to generate random numbers that meet the requirements of RNG class DRG.4:

(DRG.4.1) The internal state of the RNG uses a PTRNG of class PTG.2 as a random source.

(DRG.4.2) The RNG provides forward secrecy.

(DRG.4.3) The RNG provides backward secrecy, even if the current internal state is known.

(DRG.4.4) The RNG provides enhanced forward secrecy for every call.

(DRG.4.5)The internal state of the RNG is seeded by a PTRNG of class PTG.2.

[30] [assignment: cryptographic key destruction method]

[31] [assignment: list of standards]

(DRG.4.6) The RNG generates output for which two strings of bit length 128 are mutually different with probability 1 - 2^128.
(DRG.4.7) Statistical test suites cannot practically distinguish the random number from output sequences of an ideal RNG. The random numbers pass test procedure A as defined in [AIS20]/[AIS31].[32].

The following SFR is new and concerns cryptographic support for enhancements of [EAC2PP] (Chip Authentication 3).

- **FCS_CKM.1/CA3 Cryptographic Key Generation – Diffie-Hellman for Chip Authentication 3**

Hierarchical to:
No other components.
Dependencies:
[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] **fulfilled** by**FCS_COP.1/PACE_ENC_EAC2PP**and **FCS_COP.1/PACE_MAC_EAC2PP**

FCS_CKM.4 Cryptographic key destruction **fulfilled** by **FCS_CKM.4/EAC2PP**

FCS_CKM.1.1/CA3
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Chip Authentication 3 using Diffie Hellman[33] and specified cryptographic key sizes *256, 320, 384 and 512 bit* [34] that meet the following: [TR03110-2-v2.20] [35] .

Application note 13: After successful CA3, secure messaging (cf. FCS_COP.1/PACE_ENC_EAC2PP and FCS_COP.1/PACE_MAC_EAC2PP) is restarted using the derived session keys K_{Enc} and K_{MAC}.

- **FCS_COP.1/CA3 Cryptographic Operation – CA3**

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/CA3**

[32] [assignment: a defined quality metric]
[33] [assignment: cryptographic key generation algorithm]
[34] [assignment: *cryptographic key sizes*]
[35] [assignment: *list of standards*]

FCS_CKM.4 Cryptographic key destruction **fulfilled** by **FCS_CKM.4/EAC1_PP**

FCS_COP.1.1/CA3

The TSF shall perform the Chip Authentication 3 (CA3) protocol[36] in accordance with a specified cryptographic algorithm CA3[37] and cryptographic key sizes *256, 320, 384 and 512 bit*[38] that meet the following:[TR03110-2-v2.20][39].

Application Note 14: Whereas FCS_CKM.1/CA3 addresses the Diffie-Hellman based key-derivation, this SFR is concerned with the correct implementation and execution of the whole CA3 protocol. This in particular includes pseudonymous signature generation with **PSign** [TR03110-2-v2.20].

The following SFRs are imported due to claiming [EAC1PP]. They concern cryptographic support for applications that contain EAC1-protected data groups.

- **FCS_CKM.1/DH_PACE_EAC1PP**

Hierarchical to:

No other components.

Dependencies:

[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: **fulfilled** by FCS_CKM.2/DH.

FCS_CKM.4 Cryptographic key destruction: **fulfilled** by **FCS_CKM.4/EAC1_PP**

FCS_CKM.1.1/ DH_PACE_EAC1PP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH compliant to [*TR03111*]*[40] and specified cryptographic key sizes 256, 320, 384 and 512 bit [41,42] that meet the following: [TR03110-1][43].

- **FCS_CKM.4/EAC1_PP**

(equivalent to **FCS_CKM.4/EAC2PP**, but listed here for the sake of completeness)

[36] [assignment: *list of cryptographic operations*]
[37] [assignment: *cryptographic algorithm*]
[38] [assignment: *cryptographic key sizes*]
[39] [assignment: *list of standards*]
[40] [assignment: cryptographic key generation algorithm]
[41] [assignment: cryptographic key sizes]
[42] For length of p
[43] [assignment: list of standards]

- **FCS_COP.1/PACE_ENC_EAC1PP**

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]: **not fulfilled but justified: 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/EAC1_PP**.

FCS_COP.1.1/PACE_ENC_EAC1PP

The TSF shall perform secure messaging – encryption and decryption [44] in accordance with a specified cryptographic algorithm AES[45] in CBC mode [46] and cryptographic key sizes *128, 192 and 256* bit [47] that meet the following: compliant to [ICAOMRTDTR] [48].

Application note 15: This SFR requires the TOE to implement the cryptographic primitive AES or 3DES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the **FCS_CKM.1/DH_PACE_EAC1PP** (PACE-KEnc).

- **FCS_COP.1/PACE_MAC_EAC1PP**

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_EAC1PP**

FCS_CKM.4 Cryptographic key destruction: **fulfilled** by **FCS_CKM.4/EAC1_PP**.

FCS_COP.1.1/PACE_MAC_EAC1PP

The TSF shall perform secure messaging – message authentication code [49] in accordance with a specified cryptographic

[44] [assignment: list of cryptographic operations]

[45] [selection: *AES, 3DES*]

[46] [assignment: cryptographic algorithm]

[47] [assignment: cryptographic key sizes]/ [selection: *112, 128, 192, 256*]

[48] [assignment: list of standards]

[49] [assignment: list of cryptographic operations]

algorithm CMAC [5051] and cryptographic key sizes 128, 192 and 256 bits [52] that meet the following: compliant to [ICAOMRTDTR] [53].

Application note 16: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE_EAC1 (PACE-K_{MAC}). Note that in accordance with [ICAOMRTDTR] the (two-key) Triple-DES could be used in Retail mode for secure messaging.

- **FCS_RND.1/EAC1PP**

(equivalent to FCS_RND.1/EAC2PP, but listed here for the sake of completeness)

- **FCS_CKM.1/CA_EAC1PP**

Hierarchical to:

No other components.

Dependencies:

[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] **fulfilled** by **FCS_COP.1/PACE_ENC_EAC1PP**

FCS_CKM.4 Cryptographic key destruction **fulfilled** by **FCS_CKM.4/EAC1_PP**

FCS_CKM.1.1/CA_EAC1PP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH compliant to [TR03111][54] and specified cryptographic key sizes 256, 320, 384 and 512 bit [55] that meet the following: based on an ECDH protocol compliant to [TR03111] [56]

- **FCS_COP.1/CA_ENC_EAC1PP**

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

[50] For AES CMAC is used as a MAC mechanism.

[51] [assignment: cryptographic algorithm] / [selection: CMAC, Retail-MAC]

[52] [assignment: cryptographic key sizes]] / [selection: 112, 128, 192, 256]

[53] [assignment: list of standards]

[54] [assignment: cryptographic key generation algorithm]

[55] [assignment: cryptographic key sizes]

[56] [selection: based on the Diffie-Hellman key derivation protocol compliant to [PKCS#3] and [TR03110-1] , based on an ECDH protocol compliant to [TR03111]]

security attributes, or FCS_CKM.1 Cryptographic key generation] **fulfilled** by **FCS_CKM.1/CA_EAC1PP**

FCS_CKM.4 Cryptographic key destruction **fulfilled** by **FCS_CKM.4/EAC1_PP**

FCS_COP.1.1/CA_ENC_EAC1PP

The TSF shall perform secure messaging – encryption and decryption[57] in accordance with a specified cryptographic algorithm AES and 3DES in CBC mode[58] and cryptographic key sizes 112,128, 192 and 256 bit[59] that meet the following: **[TR03110-3]**[60].

- **FCS_COP.1/SIG_VER_EAC1PP**

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/CA_EAC1PP**

FCS_CKM.4 Cryptographic key destruction **fulfilled** by **FCS_CKM.4/EAC1_PP**

FCS_COP.1.1/SIG_VER_EAC1PP

The TSF shall perform digital signature verification[61] in accordance with a specified cryptographic algorithm ECDSA with SHA-256, SHA-384 and SHA-512 [62]and cryptographic key sizes 256, 320, 384 and 512 bit [6364]that meet the following: [TR03111] and [FIPS180-4][65].

- **FCS_COP.1/CA_MAC_EAC1PP**

Hierarchical to:

No other components.

Dependencies:

[57] [assignment: *list of cryptographic operations*]
[58] [selection: *cryptographic algorithm*]
[59] [selection: 128, 192, 256 bit]
[60] [assignment: *list of standards*]
[61] [assignment: *list of cryptographic operations*]
[62] [assignment: *cryptographic algorithm*]
[63][assignment: *cryptographic key sizes*]
[64] For length of p
[65] [assignment: *list of standards*]

[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/CA_EAC1PP**
FCS_CKM.4 Cryptographic key destruction **fulfilled** by **FCS_CKM.4/EAC1_PP**

FCS_COP.1.1/CA_MAC_EAC1PP
The TSF shall perform secure messaging – message authentication code [66] in accordance with a specified cryptographic algorithm DES Retail-MAC, AES CMAC [67]and cryptographic key sizes 112, 128,192 and 256 bits[68]that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2), TR03110-3.[69]

The following SFR is new and concerns cryptographic support for ePassport applications in combination with [EAC1PP].

- **FCS_CKM.1/CAM Cryptographic key generation – PACE-CAM public key and Diffie-Hellman for General Mapping in PACE-GM**

Hierarchical to:
No other components.

Dependencies:
[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]
fulfilled by **FCS_COP.1/PACE_ENC_EAC1PP** and **FCS_COP.1/PACE_MAC_EAC1PP**

FCS_CKM.4 Cryptographic key destruction
fulfilled by **FCS_CKM.4/EAC1_PP**

FCS_CKM.1.1/CAM
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm PACE-CAM in combination with PACE-GM[70] and specified cryptographic key sizes 256, 320, 384 and 512 bit [71]that meet the following: [ICAO9303][72].

[66] [assignment: list of cryptographic operations]
[67] [assignment: cryptographic algorithm]
[68] [assignment: cryptographic key sizes]
[69] [assignment: list of standards]
[70] [assignment: cryptographic key generation algorithm]
[71] [assignment: *cryptographic key sizes*]
[72] [assignment: *list of standards*]

Application note 17: In the combined protocol PACE-CAM, after the completion of PACE in combination with the general mapping (PACE-GM), the chip authenticates itself by adding (multiplying) the randomly chosen nonce of the GM step with the inverse of the chip authentication secret key, and sends this value together with chip authentication public key to the card; cf. [ICAO9303].

- **FCS_COP.1/CAM Cryptographic Operation – PACE-CAM**

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/CAM**

FCS_CKM.4 Cryptographic key destruction **fulfilled** by **FCS_CKM.4/EAC1_PP**

FCS_COP.1.1/CAM

The TSF shall perform the PACE-CAM protocol[73] in accordance with a specified cryptographic algorithm PACE-CAM[74] and cryptographic key sizes 256, 320, 384 and 512 bit that meet the following: [TR03110-2-v2.20][75].

Application Note 18: Whereas FCS_CKM.1/CAM addresses the Diffie-Hellman based key-derivation, this SFR is concerned with the correct implementation and execution of the whole PACE-CAM protocol. Note that in particular the last protocol step to authenticate the chip towards the terminal is an essential part of the protocol, and not addressed in FCS_CKM.1/CAM.

The following SFRs are imported due to claiming [SSCDPP]. They only concern the cryptographic support for an *eSign* application.

- **FCS_CKM.1/SSCDPP**

Hierarchical to:

No other components.

Dependencies:

[73] [assignment: list of cryptographic operations]

[74] [assignment: cryptographic algorithm]

[75] [assignment: list of standards]

[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] **fulfilled** by **FCS_COP.1/SSCDPP**

FCS_CKM.4 Cryptographic key destruction: **fulfilled** by **FCS_CKM.4/SSCDPP**

FCS_CKM.1.1/SSCDPP

The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm EC KeyGen[76] and specified cryptographic key sizes 256, 320, 384 and 512 bit[77] that meet the following: [TR03111][78].

- **FCS_CKM.4/SSCDPP**

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/SSCDPP**

FCS_CKM.4.1/SSCDPP

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the key value with zero values[79] that meets the following: none[80].

- **FCS_COP.1/SSCDPP**

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/SSCDPP**

FCS_CKM.4 Cryptographic key destruction **fulfilled** by **FCS_CKM.4/SSCDPP**

[76] [assignment: *cryptographic key generation algorithm*]
[77] [assignment: *cryptographic key sizes*]
[78] [assignment: *list of standards*]
[79] [assignment: cryptographic key destruction method]
[80] [assignment: list of standards]

FCS_COP.1.1/SSCDPP

The TSF shall perform digital signature-generation[81] in accordance with a specified cryptographic algorithm EC-DSA[82] and cryptographic key sizes 256, 320, 384 and 512 bit[83] that meet the following: [TR03111] and [FIPS180-4][84]

The following SFRs come from [MR.ED-ON-PP] :

- **FCS_COP.1/UPD_ITC_MREDONPP Cryptographic Operation – Inter Trusted Channel**

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/UPD_ITC_MREDONPP**

FCS_CKM.4 Cryptographic key destruction **fulfilled** by **FCS_CKM.4/UPD_MREDONPP**

FCS_COP.1.1/UPD_ITC_MREDONPP

The TSF shall perform secure messaging – message authentication code, encryption and decryption[85] in accordance with a specified cryptographic algorithm CMAC, AES in CBC mode[86] and cryptographic key sizes 128, 192, 256 bit[87] that meet the following: TR03110-3[88].

Application Note 19: FCS_COP.1/UPD_MREDONPP is used for the cryptographic operations needed for communication via a trusted channel as required by FTP_ITC.1/UPD.

- **FCS_CKM.1/UPD_ITC_MREDONPP Cryptographic Key Generation**

Hierarchical to:

No other components.

[81] [assignment: *list of cryptographic operations*]
[82] [assignment*: cryptographic key algorithm*]
[83] [assignment*: cryptographic key sizes*]
[84] [assignment*: list of standards*]
[85] [assignment: *list of cryptographic operations*]
[86] [assignment: *cryptographic algorithm*]
[87] [assignment: *cryptographic key sizes*]
[88] [assignment: *list of standards*]

Dependencies:

[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] fulfilled by **FCS_COP.1/UPD_ITC_MREDONPP**

FCS_CKM.4 Cryptographic key destruction fulfilled by **FCS_CKM.4/UPD_MREDONPP**

FCS_CKM.1.1/UPD_ITC_MREDONPP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH[89] and specified cryptographic key sizes 256, 320, 384 and 512 bit[90] that meet the following: [TR03111][91].

- **FCS_COP.1/UPD_DEC_MREDONPP Cryptographic Operation – Decryption of Update Packages**

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/UPD_DEC_MREDONPP**

FCS_CKM.4 Cryptographic key destruction **fulfilled** by **FCS_CKM.4/UPD_MREDONPP**

FCS_COP.1.1/UPD_DEC_MREDONPP

The TSF shall perform decryption of update packages[92] in accordance with a specified cryptographic algorithm AES in OFB mode[93] and cryptographic key sizes 256 bit[94] that meet the following: FIPS 197[95].

[89] [assignment: *cryptographic key generation algorithm*]
[90] [assignment: *cryptographic key sizes*]
[91] [assignment: *list of standards*]
[92] [assignment: list of cryptographic operations]
[93] [assignment: *cryptographic algorithm*]
[94] [assignment: *cryptographic key sizes*]
[95] [assignment: *list of standards*]

- **FCS_CKM.1/UPD_DEC_MREDONPP Cryptographic Key Generation**

Hierarchical to:

No other components.

Dependencies:

[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] **fulfilled** by **FCS_COP.1/UPD_DEC_MREDONPP**
FCS_CKM.4 Cryptographic key destruction **fulfilled** by **FCS_CKM.4/UPD_MREDONPP**

FCS_CKM.1.1/UPD_DEC_MREDONPP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH[96] and specified cryptographic key sizes 512 bits[97] that meet the following: [TR03111][98].

- **FCS_COP.1/UPD_SIG_MREDONPP Cryptographic Operation – Signature Verification of Update Packages**

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]not fulfilled but **justified**: The TOE uses security attributes (keys) that have been defined during the personalization and are fixed over the whole life time of the TOE. No import or generation of these security attributes is necessary here.

FCS_CKM.4 Cryptographic key destruction not fulfilled but **justified**: The TOE uses security attributes (keys) that have been defined during the personalization and are fixed over the whole life time of the TOE. Key destruction implies not being able to verify digital signatures from then on, and hence, is not applicable here.

FCS_COP.1.1/UPD_SIG_MREDONPP

[96] [assignment: *cryptographic key generation algorithm*]
[97] [assignment: *cryptographic key sizes*]
[98] [assignment: *list of standards*]

The TSF shall perform digital signature verification[99] in accordance with a specified cryptographic algorithm EC-DSA[100] and cryptographic key sizes 512 bit[101] that meet the following: [TR03111] and [FIPS180-4][102].

- **FCS_COP.1/UPD_INT_MREDONPP Cryptographic Operation – Integrity Verification of Update Package**

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] not fulfilled but **justified**: A hash function does not use any cryptographic key; hence, neither a respective key import nor key generation can be expected here.[103]

FCS_CKM.4 Cryptographic key destruction not fulfilled, but **justified**: A hash function does not use any cryptographic key; hence, a respective key destruction cannot be expected here.[104]

FCS_COP.1.1/UPD_INT_MREDONPP

The TSF shall perform integrity verification of update packages[105] in accordance with a specified cryptographic algorithm SHA-256 and cryptographic key sizes none[106] that meet the following: [FIPS180-4][107].

Application Note 20: Integrity verification of packages is intended to be used by the ST-Writer for a hash function (keyed or unkeyed) with which the TOE checks the integrity of received update packages prior to decryption.

[99] [assignment: *list of cryptographic operations*]
[100] [assignment: *cryptographic algorithm*]
[101] [assignment: *cryptographic key sizes*]
[102] [assignment: *list of standards*]
[103] As a hash protocol has been chosen in this iteration, the dependency to FCS_CKM.1/UPD_INT_MREDONPP defined in MR.ED-ON-PP has been deleted.
[104] As a hash protocol has been chosen in this iteration, the dependency to FCS_CKM.4/UPD_MREDONPP defined in MR.ED-ON-PP has been deleted.
[105] [assignment: *list of cryptographic operations*]
[106] [assignment: *cryptographic key sizes*]
[107] [assignment: *list of standards*]

- **FCS_CKM.1/UPD_INT_MREDONPP Cryptographic Key Generation**

Hierarchical to:

No other components.

Dependencies:

[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] **fulfilled** by **FCS_COP.1/UPD_INT_MREDONPP**

FCS_CKM.4 Cryptographic key destruction fulfilled by **FCS_CKM.4/UPD_MREDONPP**

FCS_CKM.1.1/UPD_INT_MREDONPP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm none[108] and specified cryptographic key sizes none [109] that meet the following: none[110].

Application Note 21: This SFR is intended for the key generation in case a keyed hash function is used for **FCS_COP.1/UPD_INT_MREDONPP** . In case of an unkeyed hash function, the integrity is solely implied by digital signature verification. Hence in this case, 'none' can be assigned by the ST-Writer in the above SFR.

- **FCS_CKM.4/UPD_MREDONPP Cryptographic Key Destruction**

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, orFCS_CKM.1 Cryptographic key generation]: **fulfilled** by **FCS_CKM.1/UPD_INT_MREDONPP** , **FCS_CKM.1/UPD_DEC_MREDONPP** and **FCS_CKM.1/UPD_ITC_MREDONPP**

FCS_CKM.4.1/UPD_MREDONPP

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the key value with zero values[111] that meets the following: none[112].

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

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

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

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

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

6.1.2 Class FIA

Table 3 provides an overview of the authentication and identification mechanisms used.

Name	SFR for the TOE
PACE protocol	FIA_UAU.1/PACE_EAC2PP FIA_UAU.5/PACE_EAC2PP FIA_AFL.1/Suspend_PIN_EAC2PP FIA_AFL.1/Block_PIN_EAC2PP FIA_AFL.1/PACE_EAC2PP FIA_AFL.1/PACE_EAC1PP
PACE-CAM protocol	SFRs above for the PACE part; in addition for the Chip Authentication Mapping (CAM): FIA_API.1/PACE_CAM FIA_UAU.5/PACE_EAC1PP
Terminal Authentication Protocol version 2	FIA_UAU.1/EAC2_Terminal_EAC2PP FIA_UAU.5/PACE_EAC2PP
Chip Authentication Protocol version 2	FIA_API.1/CA_EAC2PP FIA_UAU.5/PACE_EAC2PP FIA_UAU.6/PACE_EAC2PP
Terminal Authentication Protocol version 1	FIA_UAU.1/PACE_EAC1PP FIA_UAU.5/PACE_EAC1PP
Chip Authentication Protocol version 1	FIA_API.1/EAC1PP FIA_UAU.5/PACE_EAC1PP FIA_UAU.6/EAC_EAC1PP
Chip Authentication Protocol version 3	FIA_API.1/CA3 FIA_UAU.5/PACE_EAC2PP(refined) FIA_UAU.6/CA3
Restricted Identification	FIA_API.1/RI_EAC2PP
eSign-PIN	FIA_UAU.1/SSCDPP

Table 4 Overview of authentication SFRs

6.1.2.1 **SFRs for EAC2-protected Data**

The following SFRs are imported due to claiming [EAC2PP]. They mainly concern authentication mechanisms related to applications with EAC2-protected data.

- **FIA_AFL.1/Suspend_PIN_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FIA_UAU.1 Timing of authentication **fulfilled** by **FIA_UAU.1/PACE_EAC2PP**

FIA_AFL.1.1/Suspend_PIN_EAC2PP

The TSF shall detect when 2[113] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using the PIN as the shared password for PACE[114].

FIA_AFL.1.2/Suspend_PIN_EAC2PP

When the defined number of unsuccessful authentication attempts has been met[115], the TSF shall suspend the reference value of the PIN according to [TR03110-2][116].

Application Note 22: This SFR is not in conflict to FIA_AFL.1 from [PACEPP], since it just adds a requirement specific to the case where the PIN is the shared password. Thus the assigned integer number for unsuccessful authentication attempts with any PACE password could be different to the integer for the case when using a PIN.

- **FIA_AFL.1/Block_PIN_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FIA_UAU.1 Timing of authentication: **fulfilled** by **FIA_UAU.1/PACE_EAC2PP**

FIA_AFL.1.1/Block_PIN_EAC2PP

The TSF shall detect 1[117] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using the suspended[118] PIN as the shared password for PACE[119].

FIA_AFL.1.2/Block_PIN_EAC2PP

When the defined number of unsuccessful authentication attempts has been met[120], the TSF shall block the reference value of PIN according to [TR03110-2][121].

[113] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

[114] [assignment: list of authentication events]

[115] [selection: met , surpassed]

[116] [assignment: list of actions]

[117] [selection*: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values*]]

[118] As required by FIA_AFL.1/Suspend_PIN_EAC2PP

[119] [assignment: list of authentication events]

[120] [selection: met , surpassed]

[121] [assignment: list of actions]

- **FIA_API.1/CA_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_API.1.1/CA

The TSF shall provide the protocol Chip Authentication 2 according to [TR03110-2][122], to prove the identity of the TOE[123].

- **FIA_API.1/RI_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_API.1.1/RI_EAC2PP

The TSF shall provide the Restricted Identification protocol according to [TR03110-2][124], to prove the identity of the TOE[125].

Application Note 23: Restricted Identification provides a sector-specific identifier of every electronic document. It thus provides a pseudonymous way to identify the electronic document holder in a case where the CHAT of the terminal does not allow to access sensitive user data that directly identify the electronic document holder. Restricted Identification shall only be used after successfully running Terminal Authentication 2 and Chip Authentication 2. Note that Restricted Identification is optional according to [TR03110-2], and thus the above SFR only applies if Restricted Identification is supported by the TOE.

- **FIA_UID.1/PACE_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UID.1.1/PACE_EAC2PP

The TSF shall allow

1. to establish a communication channel,
2. carrying out the PACE protocol according to [TR03110-2]

[122] [assignment: authentication mechanism]

[123] [assignment: authorised user or role, or of the TOE itself]

[124] [assignment: authentication mechanism]

[125] [assignment: authorized user or role]

3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS_EAC2PP[126][127][128]
4. none[129]

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

FIA_UID.1.2/PACE_EAC2PP

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

Application Note *24*: The user identified after a successful run of PACE is a PACE terminal. In case the PIN or PUK were used for PACE, the user identified is the electronic document holder using a PACE terminal. Note that neither the CAN nor the MRZ effectively represent secrets, but are restricted-revealable; i.e. in case the CAN or the MRZ were used for PACE, it is either the electronic document

- **FIA_UID.1/EAC2_Terminal_EAC2PP**

Application note 25: The user identified after a successfully performed TA2 protocol is an EAC2 terminal. Note that TA1 is covered by FIA_UID.1/PACE_EAC1PP. In that case, the terminal identified is in addition also an EAC1 terminal.

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UID.1.1/EAC2_Terminal_EAC2PP

The TSF shall allow

1. to establish a communication channel,
2. carrying out the PACE protocol according to [TR03110-2] ,
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS_EAC2PP[130][131]
4. carrying out the Terminal Authentication protocol 2 according to [TR03110-2][132]
5. none.[133]

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

FIA_UID.1.2/EAC2_Terminal_EAC2PP

[126] The name of the SFR FMT_MTD.1/INI_DIS from EAC2PP has been adapted to the name actually used in the current ST.

[127] [assignment: list of TSF-mediated actions]

[128] In this context, it is disabled according to FMT_MTD.1/INI_DIS.

[129] [assignment: list of TSF-mediated actions]

[130] The name of the SFR FMT_MTD.1/INI_DIS from EAC2PP has been adapted to the name actually used in the current ST.

[131] In this context, it is disabled according to FMT_MTD.1/INI_DIS.

[132] [assignment: list of TSF-mediated actions]

[133] [assignment: list of TSF-mediated actions]

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

Application Note 26: The user identified after a successfully performed TA2 is an EAC2 terminal. The types of EAC2 terminals are application dependent;

Application Note 27: In the life cycle phase manufacturing, the manufacturer is the only user role known to the TOE. The manufacturer writes the initialization data and/or pre-personalization data in the audit records of the IC.
Note that a personalization agent acts on behalf of the electronic document issuer under his and the CSCA's and DS's policies. Hence, they define authentication procedures for personalization agents. The TOE must functionally support these authentication procedures. These procedures are subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role personalization agent, if a terminal proves the respective Terminal Authorization level (e. g. a privileged terminal, cf. [TR03110-2]).

- **FIA_UAU.1/PACE_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FIA_UID.1 Timing of identification **fulfilled** by **FIA_UID.1/PACE_EAC2PP**

FIA_UAU.1.1/PACE_EAC2PP

The TSF shall allow

1. to establish a communication channel,
2. carrying out the PACE protocol according to [TR03110-2]
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS_EAC2PP[134][135][136]
4. none[137]

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

FIA_UAU.1.2/PACE_EAC2PP

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

[134] The name of the SFR FMT_MTD.1/INI_DIS from EAC2PP has been adapted to the name actually used in the current ST.

[135] [assignment: list of TSF-mediated actions]

[136] In this context, it is disabled according to FMT_MTD.1/INI_DIS_EAC2PP.

[137] [assignment: list of TSF-mediated actions]

Application Note *28*: If PACE has been successfully performed, secure messaging is started using the derived session keys (PACE- K_{MAC}, PACE- K_{Enc}), cf. FTP_ITC.1/PACE. *Application Note 27* also applies here.

- **FIA_UAU.1/EAC2_Terminal_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FIA_UID.1 Timing of identification **fulfilled** by **FIA_UID.1/EAC2_Terminal_EAC2PP**

FIA_UAU.1.1/EAC2_Terminal_EAC2PP

The TSF shall allow

1. to establish a communication channel,
2. carrying out the PACE protocol according to [TR03110-2] ,
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS_EAC2PP[138][139]
4. carrying out the Terminal Authentication 2 protocol according to [TR03110-2] [140]

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

FIA_UAU.1.2/EAC2_Terminal_EAC2PP

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

Application Note 29: The user authenticated after a successful run of TA2 is an EAC2 terminal. The authenticated terminal will immediately perform Chip Authentication 2 as required by FIA_API.1/CA using, amongst other, Comp(ephem- PK_{PCD} -TA) from the accomplished TA2. Note that Passive Authentication using SO_C is considered to be part of CA2 within this ST.

- **FIA_UAU.4/PACE_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

[138] The name of the SFR FMT_MTD.1/INI_DIS from EAC2PP has been adapted to the name actually used in the current ST.

[139] In this context, it is disabled according to FMT_MTD.1/INI_DIS_EAC2PP.

[140] [assignment: list of TSF mediated actions]

No dependencies.

FIA_UAU.4.1/PACE_EAC2PP

The TSF shall prevent reuse of authentication data related to

1. PACE protocol according to [TR03110-2] ,
2. Authentication Mechanism based on AES[141]
3. Terminal Authentication 2 protocol according to [TR03110-2][142].
4. none[143]

Application Note 30: For PACE, the TOE randomly selects an almost uniformly distributed nonce of 128 bit length. The current ST supports a key derivation function based on AES; see [TR03110-2]. For TA2, the TOE randomly selects a nonce rPICC of 64 bit length, see [TR03110-2]. This SFR extends FIA_UAU.4/PACE from [PACEPP] by assigning the authentication mechanism Terminal Authentication 2

- **FIA_UAU.6/CA_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UAU.6.1/CA_EAC2PP

The TSF shall re-authenticate the user under the conditions each command sent to the TOE after a successful run of Chip Authentication 2 shall be verified as being sent by the EAC2 terminal[144].

- **FIA_AFL.1/PACE_EAC2PP**

Note here, in addition to the MRZ, the PACE password could also be a CAN or the PIN.

Hierarchical to:

No other components.

Dependencies:

FIA_UAU.1 Timing of authentication: **fulfilled** by **FIA_UAU.1/PACE_EAC2PP**

FIA_AFL.1.1/PACE_EAC2PP

The TSF shall detect when 1[145] unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password[146].

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

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

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

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

[145] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

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

FIA_AFL.1.2/PACE_EAC2PP

When the defined number of unsuccessful authentication attempts has been met[147], the TSF shall store the number of unsuccessful subsequently attempts and execute a penalty time after 5 unsuccessful attempts for each following attempt until the password is presented correctly[148,149].

Application Note 31: The open assignment operation shall be performed according to a concrete implementation of the TOE, whereby actions to be executed by the TOE may either be common for all data concerned (PACE passwords, see [ICAOMRTDTR]) or for an arbitrary subset of them or may also separately be defined for each datum in question.Since all non-blocking authorisation data (PACE passwords) being used as a shared secret within the PACE protocol do not possess a sufficient entropy[150], the TOE shall not allow a quick monitoring of its behaviour (e.g. due to a long reaction time) in order to make the first step of the skimming attack[151] requiring an attack potential beyond high, so that the threat T.Tracing can be averted in the frame of the security policy of the claimed PP.
One of some opportunities for performing this operation might be '*consecutively increase the reaction time of the TOE to the next authentication attempt using PACE passwords'*.

- **FIA_UAU.6/PACE_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UAU.6.1/PACE_EAC2PP

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.[152]

The following SFRs are new or refined from [EAC2PP] and concern cryptographic support for enhancements of [EAC2PP] (Chip Authentication 3).

[147] [selection: *met , surpassed*]

[148] [list of actions]

[149] The complete PACE process will take a very long time so that a quick monitoring of its behaviour is implicutely not possible.

[150] ≥ 100 bits; a theoretical maximum of entropy which can be delivered by a character string is N*ld(C), whereby N is the length of the string, C – the number of different characters which can be used within the string.

[151] guessing CAN or MRZ, see T.Skimming above

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

- **FIA_API.1/CA3 Authentication Proof of Identity**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_API.1.1/CA3

The TSF shall provide the protocol Chip Authentication 3 according to [TR03110-2-v2.20][153], to prove the identity of the TOE[154].

- **FIA_UAU.5/PACE_EAC2PP Multiple Authentication Mechanisms**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UAU.5.1/PACE_EAC2PP

The TSF shall provide

1. PACE protocol according to **[**TR03110-2**]** ,
2. Passive Authentication according to [ICAO9303]
3. Secure messaging ~~**in MAC-ENC mode**~~ according to **[**TR03110-3**]**
4. Symmetric Authentication Mechanism based on AES [155]
5. Terminal Authentication 2 protocol according to [TR03110-2] ,
6. Chip Authentication 2 according to [TR03110-2][156]
7. Chip Authentication 3 according to [TR03110-2-v2.20][157]
8. none[158]

to support user authentication.

FIA_UAU.5.2/PACE_EAC2PP

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 codes sent by secure messaging with the key agreed with the terminal by the PACE protocol.
2. The TOE accepts the authentication attempt as personalization agent by Symmetric Authentication Mechanism based on AES[159]
3. The TOE accepts the authentication attempt by means of the Terminal Authentication 2 protocol, only if (i) the terminal

[153] [assignment: authentication mechanism]

[154] [assignment: authorized user or role, or of the TOE itself]

[155] restricting the [selection: Triple-DES, AES or other approved algorithms]

[156] Passive Authentication using SOC is considered to be part of CA2 within this ST.

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

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

[159] [selection: *the Authentication Mechanism with Personalization Agent Key(s)*]

presents its static public key PKPCD and the key is successfully verifiable up to the CVCA and (ii) the terminal uses the PICC identifier IDPICC = Comp(ephem-PKPICC-PACE) calculated during, and the secure messaging established by the, current PACE authentication.

4. Having successfully run Chip Authentication 2, the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by Chip Authentication 2
5. Having successfully run Chip Authentication 3, the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by Chip Authentication 3[160].
6. none[161].

- **FIA_UAU.6/CA3 Re-Authenticating of Terminal by the TOE**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UAU.6.1/CA3

The TSF shall re-authenticate the user under the conditions each command sent to the TOE after a successful run of Chip Authentication 3 shall be verified as being sent by the EAC2 terminal[162].

6.1.2.2 SFRs for EAC1-protected data

The following SFRs are imported due to claiming [EAC1PP]. They mainly concern authentication mechanisms for applications with EAC1-protected data.

- **FIA_UAU.1/PACE_EAC1PP**

Hierarchical to:

No other components.

Dependencies:

FIA_UID.1 Timing of identification **fulfilled** by **FIA_UID.1/PACE_EAC1PP**.

FIA_UAU.1.1/PACE_EAC1PP

The TSF shall allow

1. to establish the communication channel,
2. carrying out the PACE Protocol according to [ICAOMRTDTR] ,

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

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

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

3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS_EAC1PP[163],[164]
4. to identify themselves by selection of the authentication key
5. to carry out the Chip Authentication Protocol Version 1 according to [TR03110-1]
6. to carry out the Terminal Authentication Protocol Version 1 according to [TR03110-1][165]
7. none[166]

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

FIA_UAU.1.2/PACE_EAC1PP

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

Application note 32: The SFR FIA_UAU.1/PACE_EAC1PP. in the current ST covers the definition in [PACEPP] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to PACEPP.

Application note 33: The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (BIS-PACE).
If PACE was successfully performed, secure messaging is started using the derived session keys (PACE- K_{MAC}, PACE- K_{Enc}), cf. FTP_ITC.1/PACE_EAC1PP.

- **FIA_UAU.4/PACE_EAC1PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UAU.4.1/PACE_EAC1PP

The TSF shall prevent reuse of authentication data related to

1. PACE Protocol according to [ICAOMRTDTR] ,

[163] The name of the SFR FMT_MTD.1/INI_DIS from EAC1PP has been adapted to the name actually used in the current ST.

[164] In this context, it is disabled according to FMT_MTD.1/INI_DIS_EAC1PP.

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

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

2. Authentication Mechanism based on AES[167]
3. Terminal Authentication Protocol v.1 according to [TR03110-1] [168].

Application note 34: The SFR FIA_UAU.4.1 in the current ST covers the definition in [PACEPP] and extends it by the EAC aspect 3. This extension does not conflict with the strict conformance to PACE PP. The generation of random numbers (random nonce) used for the authentication protocol (PACE) and Terminal Authentication as required by **FIA_UAU.4/PACE_EAC1PP** is required by FCS_RND.1 from [PACEPP].

Application note 35: The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

- **FIA_UAU.6/PACE_EAC1PP (equivalent to FIA_UAU.6/PACE_EAC2PP, but listed here for the sake of completeness)**

- **FIA_UAU.6/EAC_EAC1PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UAU.6.1/EAC_EAC1PP

The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by the Inspection System.[169]

Application note 36: The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [ICAO9303] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based

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

[168] [assignment: identified authentication mechanism(s)]

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

on a corresponding MAC algorithm whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_MAC_EAC1PP for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user.

- **FIA_API.1/EAC1PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_API.1.1/EAC1PP

The TSF shall provide a Chip Authentication Protocol Version 1 according to [TR03110-1] [170] to prove the identity of the TOE[171] .

Application note 37: This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [TR03110-1]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [ICAO9303]. The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

- **FIA_AFL.1/PACE_EAC1PP(equivalent to FIA_AFL.1/PACE_EAC2PP, but listed here for the sake of completeness)**

The following SFRs are refined from [EAC1PP]. Refinements address mainly the PACE-CAM protocol.

- **FIA_UID.1/PACE_EAC1PP Timing of identification**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UID.1.1/PACE_EAC1PP

The TSF shall allow

[170] [assignment: authentication mechanism]

[171] [assignment: authorized user or role]

1. to establish the communication channel,
2. carrying out the PACE Protocol according to **[TR03110-1]** ,
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS_EAC2PP[172][173],
4. to carry out either the Chip Authentication Protocol v.1 according to [TR03110-1] **or the Chip Authentication Mapping (PACE-CAM) according to [ICAO9303]** ,
5. to carry out the Terminal Authentication Protocol v.1 according to [TR03110-1] **resp. according to [ICAO9303] if PACE-CAM is used.[174]**
6. none[175].

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

FIA_UID.1.2/PACE_EAC1PP
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application note 38: The SFR is refined here in order for the TSF to *additionally* provide the PACE-CAM protocol by referencing [ICAO9303]. PACE-CAM combines PACE and Chip Authentication 1 for faster execution times. Hence, a TOE meeting the original requirement also meets the refined requirement.

- **FIA_UAU.5/PACE_EAC1PP Multiple authentication mechanisms**

Hierarchical to:
No other components.
Dependencies:
No dependencies.
FIA_UAU.5.1/PACE_EAC1PP
The TSF shall provide

1. PACE Protocol **and PACE-CAM protocol according to [**ICAO9303**] ,**
2. Passive Authentication according to [ICAO9303] ,
3. Secure messaging in MAC-ENC mode according to [ICAO9303],
4. Symmetric Authentication Mechanism based on AES[176]
5. Terminal Authentication Protocol v.1 according to [TR03110-1][177]

to support user authentication.

[172] The name of the SFR FMT_MTD.1/INI_DIS from **EAC2PP** has been adapted to the name actually used in the current ST.
[173] In this context, it is disabled according to FMT_MTD.1/INI_DIS.
[174] [assignment: list of TSF-mediated actions]
[175] [assignment: *list of TSF-mediated actions*]
[176] [selection: *Triple-DES, AES or other approved algorithms*]
[177] [assignment: list of multiple authentication mechanisms]

FIA_UAU.5.2/PACE_EAC1PP

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 Symmetric Authentication Mechanism based on AES.[178]
3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.
4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1 **, or if the terminal uses the public key presented during PACE-CAM and the secure messaging established during PACE**[179].
5. none[180]

Application note 39: The SFR is refined here in order for the TSF to *additionally* provide the PACE-CAM protocol by referencing [ICAO9303]. PACE-CAM combines PACE and Chip Authentication 1 for faster execution times. Hence, a TOE meeting the original requirement also meets the refined requirement.

The following SFR is newly defined in this ST and addresses the PACE-CAM protocol.

- **FIA_API.1/PACE_CAM Authentication Proof of Identity**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

[178] [selection: *the Authentication Mechanism with Personalisation Agent Key(s)*]

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

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

FIA_API.1.1/PACE_CAM
The TSF shall provide the protocol PACE-CAM [ICAO9303][181], to prove the identity of the TOE[182].

The following SFRs are imported due to claiming [SSCDPP]. They concern access mechanisms for an *eSign* application, if available.

- **FIA_UID.1/SSCDPP**

Hierarchical to:
No other components.
Dependencies:
No dependencies.
FIA_UID.1.1/SSCDPP
The TSF shall allow
1. Self test according to FPT_TST.1/SSCDPP,
2. None[183]
on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/SSCDPP
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

- **FIA_AFL.1/SSCDPP**

Hierarchical to:
No other components.
Dependencies:
FIA_UAU.1 Timing of authentication **fulfilled** by **FIA_UAU.1/PACE_EAC2PP**
FIA_AFL.1.1/SSCD Authentication failure
The TSF shall detect when 3[184] unsuccessful authentication attempts occur related to consecutive failed authentication attempts[185].
FIA_AFL.1.2/SSCD Authentication failure
When the defined number of unsuccessful authentication attempts has been met[186], the TSF shall block RAD[187].

6.1.2.3 SFRs concerning eSign-applications

[181] [assignment: authentication mechanism]
[182] [assignment: authorised user or role, or of the TOE itself]
[183] [assignment: list of additional TSF-mediated actions]
[184] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[185] [assignment: *list of authentication events*]
[186] [selection: *met* ,*surpassed*]
[187] [assignment: *list of actions*]

The next claimed SFR is refined from [SSCDPP] by additional assignments. Note that this does not violate strict conformance to [SSCDPP].

- **FIA_UAU.1/SSCDPP**

Hierarchical to:
No other components.
Dependencies:
FIA_UID.1 Timing of identification: **fulfilled** by **FIA_UID.1/SSCDPP**

FIA_UAU.1.1/SSCDPP
The TSF shall allow
1. self test according to FPT_TST.1/SSCDPP,
2. identification of the user by means of TSF required by FIA_UID.1/SSCDPP,
3. establishing a trusted channel between CGA and the TOE by means of TSF required by FTP_ITC.1/CA_EAC2PP and FTP_ITC.1/CA3 respectively,
4. establishing a trusted channel between HID and the TOE by means of TSF required by FTP_ITC.1/CA_EAC2PP and FTP_ITC.1/CA3 respectively,
5. none[188]

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

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

6.1.2.4 SFRs concerning the Post-Emission Updates

- **FIA_AFL.1/UPD_MREDONPP Update Package Verification Failure Handling**

Hierarchical to:
No other components.
Dependencies:
FIA_UAU.1 Timing of authentication: **fulfilled** by **FIA_UAU.1/UPD_MREDONPP**

FIA_AFL.1.1/UPD_MREDONPP

[188] [assignment: list of TSF mediated actions]

The TSF shall detect when 1[189] unsuccessful ~~authentication~~ **update attempts** occur~~s~~ related to authentication of the update terminal, signature verification of the update package[190].

FIA_AFL.1.2/UPD_MREDONPP

When the defined number of unsuccessful ~~authentication~~ **update attempts** has been met[191], the TSF shall abort the update, restore the state before the update attempt and return an error SW[192].

Application Note 40: The above SFR is slightly refined here by replacing 'authentication' with 'update'. Also the second assignment is made more precise. An update attempt includes authentication of the update terminal to the TOE. But when a properly authenticated terminal sends an update package that is not authentic or whose integrity cannot be validated, this is still a failed update attempt, and the TOE must handle it according to the above SFR. Hence this refinement is stricter than the original SFR definition.

- F**IA_UID.1/UPD_MREDONPP Timing of Identification**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UID.1.1/UPD_MREDONPP

The TSF shall allow

1) to establish a communication channel,
2) to authenticate an update terminal by as a TA2 terminal as defined in TR03110-2 [193]
3) none[194]

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

FIA_UID.1.2/UPD_MREDONPP

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/UPD_MREDONPP Timing of Authentication**

Hierarchical to:

No other components.

Dependencies:

[189] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] / [assignment: *positive integer number*]

[190] [assignment: *list of authentication events*]/[assignement: list of authentication events of the update procedure]

[191] [selection: *met, surpassed*]

[192] [assignment: list of actions]

[193] [assignment: cryptographic method]

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

FIA_UID.1 Timing of Identification **fulfilled** by **FIA_UID.1/UPD_MREDONPP**

FIA_UAU.1.1/UPD_MREDONPP

The TSF shall allow

1) to establish a communication channel,
2) to authenticate an update terminal ~~by~~ as a TA2 terminal as defined in TR03110-2 [195]
3) none[196]

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

FIA_UAU.1.2/UPD_MREDONPP

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

6.1.3 Class FDP

Multiple iterations of FDP_ACF.1 exist from imported PPs to define the access control SFPs for (common) user data, EAC1-protected user data, and EAC2-protected user data. The access control SFPs defined in FDP_ACF.1/EAC1PP from [EAC1PP] and FDP_ACF.1/EAC2PP from [EAC2PP] are here unified to one single FDP_ACF.1/TRM, whereas the several iterations of FDP_ACF.1 from [SSCDPP] stand separate. Here we take FDP_ACF.1/EAC2PP as a base definition of functional elements, and it is refined in a way that it is compatible with FDP_ACF.1/EAC1PP. Hence highlighting refers to changes w.r.t. to FDP_ACF.1/EAC2PP. In the application note below, we explain how FDP_ACF.1/EAC1PP is covered as well.

Concerning FDP_ACF.1/TRM here and the several iterations FDP_ACF.1 from [SSCDPP], we remark that FDP_ACF.1/TRM also concerns data and objects for signature generation. Note however, that FDP_ACF.1/TRM requires that *prior* to granting access to the signature application, in which the access controls defined in [SSCDPP] apply, an EAC2 terminal and the electronic document holder need to be authenticated. Hence, no inconsistency exist.

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

Hierarchical to:

No other components.

Dependencies:

[195] [assignment: cryptographic method]

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

FDP_ACC.1 Subset access control **fulfilled** by **FDP_ACC.1/TRM_EAC1PP** and **FDP_ACC.1/TRM_EAC2PP**

FMT_MSA.3 Static attribute initialization not fulfilled, but **justified:** The access control TSF according to FDP_ACF.1/TRM uses security attributes having been defined during the personalization 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[197] to objects based on the following:

1) Subjects:
   a) Terminal,
   b) PACE terminal ,
   c) EAC2 terminal *(IS,AT, ST)*[198] ,
   d) EAC1 terminal [199] ;
2) Objects:
   a) all user data stored in the TOE; including sensitive **EAC1-protected user data, and sensitive EAC2-protected** user data.
   b) all TOE intrinsic secret (cryptographic) data
3) Security attributes:
   a) Terminal Authorization Level (access rights)
   b) Authentication status of the electronic document holder as a signatory (if an eSign application is included)[200][201].

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:A PACE terminal is allowed to read data objects from FDP_ACF.1/TRM after successful PACE authentication according to [TR03110-2] **and/or [**ICAO9303**]** , as required by FIA_UAU.1/PACE.[202]

FDP_ACF.1.3/TRM

---

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

[198] [assignment: *list of EAC2 terminal types*]

[199] [assignment: list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or name groups of SFP-relevant security attributes] (added using open assignment of [EAC2PP])

[200] [assignment: list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or name groups of SFP-relevant security attributes] (added using open assignment of [EAC2PP])

[201] [assignment: list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or name groups of SFP-relevant security attributes] (all bullets in FDP_ACF.1.1/TRM w.r.t. [CC2])

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

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.[203]
FDP_ACF.1.4/TRM
The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
1. Any terminal not being ~~authenticated as~~ a PACE terminal or an EAC2 terminal **or an EAC1 terminal** is not allowed to read, to write, to modify, or to use any user data stored on the electronic document. [204]
2. Terminals not using secure messaging are not allowed to read, write, modify, or use any data stored on the electronic document.
3. No subject is allowed to read 'Communication Establishment Authorization Data' stored on the electronic document
4. No subject is allowed to write or modify 'secret electronic document holder authentication data' stored on the electronic document, except for PACE terminals or EAC2 terminals executing PIN management based on the following rules: Change PIN, Resume PIN, Unblock PIN, Activate PIN, Deactivate PIN[205].
5. No subject is allowed to read, write, modify, or use the private Restricted Identification key(s) and Chip Authentication key(s) stored on the electronic document.
6. Reading, modifying, writing, or using sensitive user data **that are protected only by EAC2, is allowed only** to EAC2 terminals using the following mechanism:The TOE applies the EAC2 protocol (cf. **FIA_UAU.5/PACE_EAC2PP**) to determine access rights of the terminal according to [TR03110-2] . To determine the effective authorization of a terminal, the chip must calculate a bitwise Boolean 'and' of the relative authorization contained in the CHAT of the Terminal Certificate, the referenced DV Certificate, and the referenced CVCA Certificate, and additionally the confined authorization sent as part of PACE. Based on that effective authorization and the terminal type drawn from the CHAT of the Terminal Certificate, the TOE shall grant the right to read, modify or write sensitive user data, or perform operations using these sensitive user data.
7. No subject is allowed to read, write, modify or use the data objects 2b) of FDP_ACF.1.1/TRM.
8. No subject is allowed to read sensitive user data that are protected only by EAC1, except an EAC1 terminal (OID inspection system) after EAC1, cf. FIA_UAU.1/EAC1, that has a corresponding relative authorization level. This includes in particular EAC1-protected user data DG3 and DG4 from an ICAO-compliant ePass application, cf. [TR03110-1] and [ICAO9303] .
9. If sensitive user data is protected both by EAC1 and EAC2, no subject is allowed to read those data except EAC1 terminals or

[203] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]
[204] note that authentication of an EAC1 or EAC2 terminal to a TOE in certified mode implies a prior run of PACE.
[205] [assignment: *list of rules for PIN management chosen from [TR03110-2]*]

EAC2 terminals that access these data according to rule 6 *or* rule 8 above.
10. Nobody is allowed to read the private signature key(s). [206]

Application note 41: The above definition is based on FDP_ACF.1/TRM_EAC2PP. We argue that it covers FDP_ACF.1/TRM_EAC1PP as well. Subject 1b and 1d are renamed here from FDP_ACF.1.1/TRM_EAC1PP according to Table 1. Objects in 2), in particular the term *EAC1-protected user data*, subsume all those explicitly enumerated in FDP_ACF.1.1/TRM_EAC1PP. Also the security attribute 3a) *Terminal Authorization Level* here subsumes the explicitly enumerated attributes 3a) and 3b) of FDP_ACF.1.1/TRM_EAC1PP, but are semantically the same. Since in addition EAC2 protected data are stored in the TOE of this ST, additional subjects, objects and security attributes are listed here. However since they apply to data with a different protection mechanism (EAC2), strict conformance is not violated.
FDP_ACF.1.2/TRM uses the renaming of Table 1, and references in addition [TR03110-2]. However the references are compatible as justified in [EAC2PP], yet both are mentioned here since [TR03110-2] is the primary norm for an eID application, whereas [ICAO9303] is normative for an ICAO compliant ePass application. Investigating the references reveals that access to data objects defined in FDP_ACF.1.1/TRM must be granted if these data are neither EAC1-protected, nor EAC2-protected.
FDP_ACF.1.3/TRM is the same as in FDP_ACF.1.3/TRM_EAC2PP.References are changed in FDP_ACF.1.2/TRM_EAC1PP. It is already justified in [EAC2PP] that definitions in [TR03110-2] and [ICAO9303] are compatible.
FDP_ACF.1.3/TRM is taken over from [EAC1PP] and [EAC2PP] (same formulation in both).Rules 1 and 2 of FDP_ACF.1.4/TRM_EAC1PP in [EAC1PP] are covered by their counterparts rule 1 and rule 2 here. Rules 3 and 4, and rule 6 of FDP_ACF.1.4/TRM_EAC1PP in [EAC1PP] are combined here to rule 8, where terminals need the corresponding CHAT to read data groups. Rule 5 of [EAC1PP] is here equivalent to rule 7. None of this conflicts with strict conformance to [EAC1PP]. Note that adding additional rules compared to FDP_ACF.1.4/TRM_EAC1PP here can never violate strict conformance, as these are rules that explicitly *deny* access of subjects to objects. Hence security is always increased.
The above definition also covers FDP_ACF.1.1/TRM_EAC2PP and extends it by additional subjects and objects. Sensitive user data in the definition of FDP_ACF.1.1/TRM_EAC2PP are here EAC2-protected sensitive user data. EAC1-protected data are added here by refinement. Since the protection level and mechanisms w.r.t. to EAC2-protected data do not change, strict conformance is not violated.

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

FDP_ACF.1.2/TRM_EAC2PP and FDP_ACF.1.3/TRM_EAC2PP are equivalent to the current definition. Rules 8, 9 and 10 are added here by open assignment from [EAC2PP]. None of this conflicts with strict conformance.
The dependency of this SFR is met by FDP_ACC.1/TRM_EAC1PP and FDP_ACC.1/TRM_EAC2PP. Note that the SFR in [EAC1PP] applies the assignment operation, whereas in [EAC2PP] (by referencing [PACEPP]) the assignment is left open. Hence they are compatible. We remark that in order to restrict the access to user data as defined in the SFR FDP_ACC.1/TRM_EAC1PP, clearly access to objects 2b) of FDP_ACF.1.1/TRM must be restricted as well according to the SFP, otherwise access to user data is impossible to enforce.

The following SFRs are imported due to claiming [EAC2PP]. They concern access control mechanisms related to EAC2-protected data.

- **FDP_ACC.1/TRM_EAC2PP This SFR is equivalent to/covered by FDP_ACC.1/TRM_EAC1PP ; cf. the application note above.**

- **FDP_ACF.1/TRM_EAC2PP This SFR is equivalent to/covered by FDP_ACF.1/TRM**

- **FDP_RIP.1/EAC2PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FDP_RIP.1.1/EAC2PP

The TSF shall ensure that any previous information content of a resource is made unavailable upon *the deallocation of the resource from*[207] the following objects:

1. Session keys (PACE-K_{MAC}, PACE-K_{Enc}), (CA-K_{MAC}, CA-K_{Enc})(immediately after closing related communication session),
2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret K),
3. secret electronic document holder authentication data, e.g. PIN and/or PUK(when their temporarily stored values are not used any more),
4. the private Restricted Identification key SK_{ID}[208].

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

[208] [assignment: list of (further) objects]

Application note 42: Note that the formulation *session keys* in the above SFR MUST be interpreted here to include CA3 ephemeral and session keys as well.

- **FDP_UCT.1/TRM_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

[FTP_ITC.1 Inter-TSF trusted channel, orFTP_TRP.1 Trusted path] **fulfilled** by **FTP_ITC.1/PACE_EAC2PP**

[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] **fulfilled** by **FDP_ACC.1/TRM_EAC2PP**

FDP_UCT.1.1/TRM

The TSF shall enforce the Access Control SFP [209] to be able to transmit and receive [210] user data in a manner protected from unauthorised disclosure.

- **FDP_UIT.1/TRM_EAC2PP**

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_EAC2PP**

[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] **fulfilled** by **FDP_ACC.1/TRM_EAC2PP**

FDP_UIT.1.1/TRM_EAC2PP

The TSF shall enforce the Access Control SFP[211] to be able to transmit and receive [212] user data in a manner protected from modification, deletion, insertion and replay [213] errors.

FDP_UIT.1.2/TRM_EAC2PP

The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay [214] has occurred.

The following SFRs are imported due to claiming [EAC1PP]. They concern access control mechanisms related to EAC1-protected data.

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

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

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

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

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

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

- **FDP_ACC.1/TRM_EAC1PP The above is equivalent to FDP_ACC.1/TRM_EAC2PP, since EF.SOD (cf. FDP_ACC.1/TRM in [EAC1PP]) can be considered user data.; cf. also the application note below FDP_ACF.1/TRM.**

- **FDP_ACF.1/TRM_EAC1PP The above is covered by FDP_ACF.1/TRM; cf. Application Note there.**

- **FDP_RIP.1/EAC1PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FDP_RIP.1.1/EAC1PP

The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from*[215] 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[216]),
3. none[217].

- **FDP_UCT.1/TRM_EAC1PP** (equivalent to FDP_UCT.1/TRM_EAC2PP, but listed here for the sake of completeness)
- **FDP_UIT.1/TRM_EAC1PP** (equivalent to FDP_UIT.1/TRM_EAC2PP, but listed here for the sake of completeness)

The following SFRs are imported due to claiming [SSCDPP]. They concern access control mechanisms of an *eSign* application.

- **FDP_ACC.1/SCD/SVD_Generation_SSCDPP**

Hierarchical to:

No other components.

Dependencies:

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

[216] According to [TR03110-1]

[217] [assignment: list of (further) objects]

FDP_ACF.1 Security attribute based access control **fulfilled** by **FDP_ACF.1/Signature-creation_SSCDPP**

FDP_ACC.1.1/ SCD/SVD_Generation_SFP_SSCD

The TSF shall enforce the SCD/SVD_Generation_SFP[218] on

1. subjects: S.User,
2. objects: SCD, SVD,
3. operations: generation of SCD/SVD pair[219].

- **FDP_ACF.1/SCD/SVD_Generation_SSCDPP**

Hierarchical to:

No other components.

Dependencies:

FDP_ACC.1 Subset access control **fulfilled** by **FDP_ACC.1/Signature-creation_SSCDPP**

FMT_MSA.3 Static attribute initialisation **fulfilled** by **FMT_MSA.3/SSCDPP**

FDP_ACF.1.1/SCD/SVD_Generation_SSCDPP

The TSF shall enforce the SCD/SVD_Generation_SFP[220] to objects based on the following: the user S.User is associated with the security attribute "SCD / SVD Management "[221].

FDP_ACF.1.2/SCD/SVD_Generation_SSCDPP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: S.User with the security attribute "SCD / SVD Management" set to "authorised" is allowed to generate SCD/SVD pair[222].

FDP_ACF.1.3/SCD/SVD_Generation_SSCDPP

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[223].

FDP_ACF.1.4/SCD/SVD_Generation_SSCDPP

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

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

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

[221] [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*]

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

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

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

S.User with the security attribute “SCD / SVD management” set to “not authorised” is not allowed to generate SCD/SVD pair[224].

- **FDP_ACC.1/SVD_Transfer_SSCDPP**

Hierarchical to:

No other components.

Dependencies:

FDP_ACF.1 Security attribute based access control **fulfilled** by **FDP_ACF.1/Signature-creation_SSCDPP**

FDP_ACC.1.1/ SVD_Transfer_SSCDPP

The TSF shall enforce the SVD_Transfer_SFP[225] on

1 subjects: S.User,

2 objects: SVD

3 operations: export[226].

- **FDP_ACF.1/SVD_Transfer_SSCDPP**

Hierarchical to:

No other components.

Dependencies:

FDP_ACC.1 Subset access control **fulfilled** by **FDP_ACC.1/Signature-creation_SSCDPP**
FMT_MSA.3 Static attribute initialisation **fulfilled** by **FMT_MSA.3/SSCDPP**

FDP_ACF.1.1/SVD_Transfer_SSCDPP

The TSF shall enforce the SVD_Transfer_SFP[227] to objects based on the following:

1 the S.User is associated with the security attribute Role,

2 the SVD [228].

FDP_ACF.1.2/SVD_Transfer_SSCDPP

[224] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[225] [assignment: *access control SFP*]
[226] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[227] [assignment: *access control SFP*]
[228] [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*]

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *R.Admin* is allowed to export SVD[229].

FDP_ACF.1.3/ SVD_Transfer_SSCDPP

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[230].

FDP_ACF.1.4/SVD_Transfer_SSCDPP

The TSF shall explicitly deny access of subjects to objects based on the rule: none[231].

- **FDP_ACC.1/Signature-creation_SSCDPP**

Hierarchical to:

No other components.

Dependencies:

FDP_ACF.1 Security attribute based access control **fulfilled** by **FDP_ACF.1/Signature-creation_SSCDPP**

FDP_ACC.1.1/ Signature-creation_SSCDPP

The TSF shall enforce the Signature-creation_SFP[232] on

1. subjects: S.User,
1. objects: DTBS/R, SCD,
2. operations: signature-creation.[233]

- **FDP_ACF.1/Signature-creation_SSCDPP**

Hierarchical to:

No other components.

Dependencies:

FDP_ACC.1 Subset access control **fulfilled** by **FDP_ACC.1/SCD/SVD_Generation_SSCDPP**

FMT_MSA.3 Static attribute initialization fulfilled by **FMT_MSA.3/SSCDPP**

FDP_ACF.1.1/Signature-creation_SSCDPP

The TSF shall enforce the Signature-creation_SFP[234] to objects based on the following:

(1) the user S.User is associated with the security attribute “Role” and

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

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

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

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

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

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

(2) the SCD with the security attribute “SCD Operational”[235].

FDP_ACF.1.2/Signature-creation_SSCDPP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
R.Sigy is allowed to create digital signatures for DTBS/R with SCD which security attribute “SCD operational” is set to “yes”[236].

FDP_ACF.1.3/Signature-creation_SSCDPP

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[237].

FDP_ACF.1.4/Signature-creation_SSCDPP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
S.User is not allowed to create digital signatures for DTBS/R with SCD which security attribute “SCD operational” is set to “no”[238].

- **FDP_RIP.1/SSCDPP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FDP_RIP.1.1/SSCDPP

The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from[239] the following objects: SCD[240].

- **FDP_SDI.2/Persistent_SSCDPP**

Hierarchical to:

FDP_SDI.1 Stored data integrity monitoring.

Dependencies:

No dependencies.

FDP_SDI.2.1/ Persistent_SSCDPP

The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[241] on all objects, based on the following attributes: integrity checked stored data[242].

FDP_SDI.2.2/ Persistent_SSCDPP

---

[235] [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*]

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

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

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

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

[240] [assignment: *list of objects*]

[241] [assignment: *integrity errors*]

[242] [assignment: *user data attributes*]

Upon detection of a data integrity error, the TSF shall

1. prohibit the use of the altered data
2. inform the S.Sigy about integrity error[243].

- **FDP_SDI.2/DTBS_SSCDPP**

Hierarchical to:

FDP_SDI.1 Stored data integrity monitoring.

Dependencies:

No dependencies.

FDP_SDI.2.1/DTBS_SSCDPP

The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[244] on all objects, based on the following attributes: integrity checked stored DTBS[245].

FDP_SDI.2.2/DTBS_SSCDPP

Upon detection of a data integrity error, the TSF shall

1. prohibit the use of the altered data
2. inform the S.Sigy about integrity error[246].

The following SFRs are imported due to claiming [MR.ED-ON-PP]. They concern access control mechanisms of post-emission updates.

- **FDP_ACC.1/UPD_MREDONPP Subset Access Control – Terminal Access**

Hierarchical to:

No other components.

Dependencies:

FDP_ACF.1 Security attribute based access control: **fulfilled** by **FDP_ACF.1/UPD_MREDONPP**

FDP_ACC.1.1/UPD_MREDONPP

The TSF shall enforce the Update Access Control SFP[247] on

1) Subjects:
   a) terminal,
   b) update terminal.
2) Objects:

[243] [assignment: *action to be taken*]
[244] [assignment: *integrity errors*]
[245] [assignment: *user data attributes*]
[246] [assignment: *action to be taken*]
[247] [assignment: *access control SFP*]

a) version information identifying the TOE software

b) update package

c) update log information

3) Operations:

a) reading out version information,

b) reading out log data,

c) uploading an update package on the TOE, or

d) initiating an update procedure[248]

and none[249].

- **FDP_ACF.1/UPD_MREDONPP Security Attribute based Access Control – Terminal Access**

Hierarchical to:

No other components.

Dependencies:

FDP_ACC.1 Subset access control **fulfilled** by **FDP_ACC.1/UPD_MREDONPP**

FMT_MSA.3 Static attribute initialization not fulfilled, but **justified**: The access control TSF according to FDP_ACF.1/UPD uses security attributes that have been defined during personalization, and that are 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/UPD_MREDONPP

The TSF shall enforce the Update Access Control SFP[250] to objects based on the following:

1) Subjects:

a) terminal,

b) update terminal

2) Objects:

a) version information identifying the TOE software

b) update package

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

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

[250] [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]]

c) update log information

3) Security attributes:

a) access rights

4) none[251].

FDP_ACF.1.2/UPD_MREDONPP

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

The authentication level of a terminal must be determined by TR03110-2[252]as required by FIA_UAU.1/UPD_MREDONPP. Depending on the authentication level, an authenticated update terminal is allowed one or more of the following:

- read one or more data objects from FDP_ACF.1/UPD_MREDONPP
- upload an update package to the TOE and initiate the update procedure.

The precise definition of access rights and how the authentication level is calculated from an authenticated terminal is defined in TR03110-2-v2.20 and TR03111[253][254].

FDP_ACF.1.3/UPD_MREDONPP

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.[255]

FDP_ACF.1.4/UPD_MREDONPP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:none[256].

- **FDP_IFC.1/UPD_MREDONPP Subset information flow control**

Hierarchical to:

No other components.

Dependencies:

[251] [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*]

[252] [assignment: list of technical specifications of cryptographic procedures]

[253] [assignment: list of technical specifications of cryptographic procedures]

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

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

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

FDP_IFF.1 Simple security attributes, **fulfilled** by **FDP_IFF.1/UPD_MREDONPP**

FDP_IFC.1.1/UPD_MREDONPP:

The TSF shall enforce the Update Flow Control SFP[257] on the following:

1) Subjects:
   a) terminal,
   b) update terminal.
2) information:
   a) update package
   b) update data
   c) meta-data, such as version information
3) operations:
   a) performing an update[258].

- **FDP_IFF.1/UPD_MREDONPP Simple Security Attributes**

Hierarchical to:

No other components.

Dependencies:

FDP_IFC.1 Subset information flow control: **fulfilled** by FDP_IFC.1/UPD

FMT_MSA.3 Static attribute initialization:not fulfilled, but **justified:** The update control TSF according to FDP_IFF.1/UPD uses security attributes that have been defined during personalization, and that are 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_IFF.1.1/UPD_MREDONPP

The TSF shall enforce the Update Control SFP[259] based on the following types of subject and information security attributes:

1) Subjects:
   a) terminal,
   b) update terminal.
2) information:

[257] [assignment: *information flow control SFP*]

[258] [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]

[259] [assignment: *information flow control SFP*]

a) update package

b) update data

c) meta-data, such as version information

3) security attributes:

a) update package verification status with the values: NOT VERIFIED (default status), SUCCESSFULLY VERIFIED, and VERIFICATION FAILED[260].

FDP_IFF.1.2/UPD_MREDONPP

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1. The terminal has established a secure channel with the TOE.

2. The TOE shall only accept update packages sent via a secure channel established with an authenticated update terminal[261].

FDP_IFF.1.3/UPD_MREDONPP

The TSF shall enforce the following rules in their specific order:

1) The integrity (using the keyed or unkeyed hash function cf. FCS_COP.1/UPD_INT) and authenticity (using the digital signature, cf. FCS_COP.1/UPD_SIG) of the first part of the update package is verified. If the integrity and authenticity are not both validated, abort with VERIFICATION FAILED, and erase all data transferred so far, cf. FDP_RIP.1.

2) The first part of the update package is only decrypted, cf. FCS_COP.1/UPD_DEC, if the integrity and authenticity of the that part has been verified in rule 1. If the decryption fails, abort with VERIFICATION FAILED, and erase all data transferred so far, cf. FDP_RIP.1.

3) If all parts of the update package have been decrypted, continue with rule 4. Otherwise, apply rules 1. and 2. on the remaining parts (replace 'first part' with 'current part' above) until either all parts have been decrypted, or the procedure has been aborted with VERIFICATION FAILED.

4) If additional meta-data is stored in the update package none[262] is not verified as correct according to none [263] the security attribute is set to VERIFICATION FAILED and the update package including all associated

[260] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

[261] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]

[262] [assignment: list of meta-data contained in the update package or reference to technical specification(s) defining those]

[263] [assignment*: technical specification(s) defining correct form and content of meta-data*]

data are destroyed, cf. FDP_RIP.1. Correctness w.r.t. the referenced technical specification must not contradict any of the given rules here.

5) Next, the TSF shall verify that:

a) the version number of the update package must be greater than the version of the installed corresponding software package;

b) the update data are suitable to the specific TOE configuration/platform by checking relevant meta-data (i.e. TOE product identifier, version number etc.).

If all conditions in step 5 are verified, the verification status is set to SUCCESSFULLY VERIFIED. Otherwise abort with VERIFICATION FAILED, and erase all data transferred so far, cf. FDP_RIP.1.

Only if the verification status is SUCCESSFULLY VERIFIED, the TOE shall install the update data[264].

FDP_IFF.1.4/UPD_MREDONPP

The TSF shall explicitly authorize an information flow based on the following rules: HUiF[265].

FDP_IFF.1.5/UPD_MREDONPP

The TSF shall explicitly deny an information flow based on the following rules: HUiF[266].

- **FDP_RIP.1/UPD_MREDONPP Subset Residual Information Protection**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FDP_RIP.1.1/UPD_MREDONPP

The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from*[267] the following objects:

1) session keys (immediately after closing related communication session),

2) all ephemeral keys needed for ECIES related to the update mechanism.

[264] [assignment: *additional information flow control SFP rules*]

[265] [assignment: *rules, based on security attributes, that explicitly authorize information flows*]

[266] [assignment: *rules, based on security attributes, that explicitly deny information flows]*

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

3) Update package, decrypted update data and meta-data uploaded to the TOE or generated during the update procedure[268].

4) none[269].

Application Note 43: The functional family FDP_RIP possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1 requires a certain quality metric ('any previous information content of a resource is made unavailable') for key destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard. The ST-Writer should in particular list all relevant ephemeral keys required for the update procedure or reference a technical specification that defines the related protocols and generated ephemeral keys.

6.1.4 Class FTP

The following SFRs are imported from [EAC2PP].

- **FTP_ITC.1/PACE_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FTP_ITC.1.1/PACE_EAC2PP

The TSF shall provide a communication channel between itself ~~and another trusted IT product~~ **a PACE terminal** 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. **The trusted channel shall be established by performing the PACE protocol according to [TR03110-2].**

FTP_ITC.1.2/PACE_EAC2PP

The TSF shall permit **~~another trusted IT product~~ a PACE terminal** [270] to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE_EAC2PP

The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and a **PACE terminal after PACE**. [271]

[268] [assignment: *list of objects*]

[269] [assignment: *list of objects*]

[270] [selection: *the TSF, another trusted IT product*]

[271] [assignment: *list of functions for which a trusted channel is required*]

- **FTP_ITC.1/CA_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FTP_ITC.1.1/CA_EAC2PP Inter-TSF trusted channel after CA

The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **an EAC2 terminal** 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. **The trusted channel shall be established by performing the CA2 protocol according to [**TR03110-2**].**

FTP_ITC.1.2/CA_EAC2PP Inter-TSF trusted channel after CA

The TSF shall permit **~~another trusted IT product~~ an EAC2 terminal**[272] to initiate communication via the trusted channel.

FTP_ITC.1.3/CA_EAC2PP Inter-TSF trusted channel after CA

The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and an EAC2 terminal after Chip Authentication 2.[273]

- **FTP_ITC.1/CA3 Inter-TSF trusted channel after CA3**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FTP_ITC.1.1/CA3

The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **an EAC2 terminal** 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. **The trusted channel shall be established by performing the CA3 protocol according to [TR03110-2-v2.20].**

FTP_ITC.1.2/CA3

[272] [selection: the TSF, another trusted IT product]

[273] [assignment: list of functions for which a trusted channel is required]

The TSF shall permit ~~another trusted IT product~~ **an EAC2 terminal** [274] to initiate communication via the trusted channel.

FTP_ITC.1.3/CA3

The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and an EAC2 terminal after Chip Authentication 3. [275]

The following SFR is imported due to claiming [EAC1PP]. It concerns applications with EAC1-protected data.

- **FTP_ITC.1/PACE_EAC1PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FTP_ITC.1.1/PACE_EAC1PP

The TSF shall provide a communication channel between itself and **PACE terminal (PCT) after PACE** 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_EAC1PP

The TSF shall permit **the PCT**[276] to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE_EAC1PP

The TSF shall **enforce** communication via the trusted channel for any data exchange between the TOE and the PCT after PACE.[277]

The following SFR is imported from [MR.ED-ON-PP].

- **FTP_ITC.1/UPD_MREDONPP Inter-TSF trusted Channel**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FTP_ITC.1.1/UPD_MREDONPP

[274] [selection: the TSF, another trusted IT product]

[275] [assignment: *list of functions for which a trusted channel is required*]

[276] [selection: the TSF, another trusted IT product]

[277] [assignment: list of functions for which a trusted channel is required]

The TSF shall provide a communication channel between itself ~~and another trusted IT product~~ **an update terminal** 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/UPD_MREDONPP

The TSF shall ~~permit another trusted IT product~~ **an update terminal** to initiate communication via the trusted channel.

FTP_ITC.1.3/UPD_MREDONPP

The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the update terminal.[278]

6.1.5 Class FAU

The following SFR is imported due to claiming [EAC2PP]. It concerns applications with EAC2-protected data.

- **FAU_SAS.1/EAC2PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FAU_SAS.1.1

The TSF shall provide the Manufacturer[279] with the capability to store the Initialisation and Pre-Personalisation Data[280] in the audit records.

The following SFR is imported due to claiming [EAC1PP]. It concerns applications with EAC1-protected data.

- **FAU_SAS.1/EAC1PP (equivalent to FAU_SAS.1/EAC2PP, but listed here for the sake of completeness)**

The following SFR is imported from [MR.ED-ON-PP].

[278] [assignment: *list of functions for which a trusted channel is required*]

[279] [assignment: *authorised users*]

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

- **FAU_SAS.1/UPD_MREDONPP Audit Storage of Update History**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FAU_SAS.1.1/UPD_MREDONPP

The TSF shall provide **the TOE update functionality** with the capability to store update log information and version history, namely the following data objects: BZ(number of patch installation tries), FS (return code), FP (return additional information), ZPV(patch-version to be installed), L.CHR (length of CHR), CHR (Certificate Holder Reference)[281][282] in the audit records.

Justification: According to [CC1], a PP author is allowed to refine an SFR to apply to some, but not all subjects. The refinement of this SFR is such an exception, since the TOE update functionality is technically not an authorized user. Hence, the refinement is justified.Note FAU_SAS.1 from [MR.ED2.0] applies as well. The SFR here is a new iteration refining the definition of [CC2] and is only concerned with the TOE update functionality.

6.1.6 Class FMT

- **FMT_SMR.1 Security roles**

Hierarchical to:

No other components.

Dependencies:

FIA_UID.1 Timing of identification: **fulfilled** by **FIA_UID.1/PACE_EAC1PP**, **FIA_UID.1/PACE_EAC2PP**, **FIA_UID.1/EAC2_Terminal_EAC2PP**, see also the Application Note below.

FMT_SMR.1.1

The TSF shall maintain the roles

1. Manufacturer ,
2. Personalization Agent,
3. Country Verifying Certification Authority,
4. Document Verifier,
5. Terminal,
6. PACE terminal ,

[281] [assignment: *list of update log information data*]

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

7. EAC2 terminal , if the eID, ePassport and/or eSign application are active ,
8. EAC1 terminal , if the ePassport application is active
9. Electronic document holder.[283]

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

The next SFRs are imported from [EAC2PP]. They concern mainly applications with EAC2-protected data.

- **FMT_MTD.1/CVCA_INI_EAC2PP**

Hierarchical to:
No other components.
Dependencies:
FMT_SMF.1 Specification of management functions: **fulfilled** by **FMT_SMF.1/EAC2PP**

FMT_SMR.1 Security roles: **fulfilled** by **FMT_SMR.1**

FMT_MTD.1.1/CVCA_INI_EAC2PP
The TSF shall restrict the ability to write[284] the

1. initial Country Verifying Certification Authority Public Key (PK_{CVCA}),
2. metadata of the initial Country Verifying Certification Authority Certificate (C_{CVCA}) as required in [TR03110-2], resp [TR03110-3]
3. initial Current Date,
4. none[285]

to the Personalisation Agent[286].

- **FMT_MTD.1/CVCA_UPD_EAC2PP**

Hierarchical to:
No other components.
Dependencies:
FMT_SMF.1 Specification of management functions: **fulfilled** by **FMT_SMF.1/EAC2PP**

FMT_SMR.1 Security roles: **fulfilled** by **FMT_SMR.1**

FMT_MTD.1.1/CVCA_UPD_EAC2PP
The TSF shall restrict the ability to update[287] the

1. Country Verifying Certification Authority Public Key (PK_{CVCA}),

[283] [assignment: the authorized identified roles]
[284] selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[285] [assignement. List of TSF data]
[286] [assignment: the authorised identified roles]/ [selection: the manufacturer, the personalization agent]
[287] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]

2. metadata of the Country Verifying Certification Authority Certificate (C_{CVCA}) as required by [TR03110-2], resp. TR03110-3,
3. none[288].

to Country Verifying Certification Authority[289].

- **FMT_SMF.1/EAC2PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies

FMT_SMF.1.1/EAC2PP

The TSF shall be capable of performing the following management functions:

1. Initialisation,
2. Personalisation,
3. Configuration,
4. Resume and unblock the eID-PIN[290],
5. Activate and deactivate the eID-PIN[291].

- **FMT_SMR.1/PACE_EAC2PP** This SFR is combined with MT_SMR.1/PACE_EAC1PP into FMT_SMR.1.
- **FMT_MTD.1/DATE_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions: fulfilled by **FMT_SMF.1/EAC2PP**

FMT_SMR.1 Security roles: fulfilled by **FMT_SMR.1/PACE_EAC2PP**

FMT_MTD.1.1/DATE

The TSF shall restrict the ability to modify[292] the Current Date[293] to

1. Country Verifying Certification Authority,
2. Document Verifier,

[288] [assignment: list of TSF data]

[289] [assignment: the authorised identified roles]

[290] unblocking eSign-PIN is managed by FMT_SMF.1/SSCD

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

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

[293] [assignment: list of TSF data]

3. EAC2 terminal (IS, AT, ST[294]) possessing an Accurate Terminal Certificate according to [TR03110-3][295].
4. none[296]

- **FMT_MTD.1/PA_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions fulfilled by **FMT_SMF.1/EAC2PP**

FMT_SMR.1 Security roles fulfilled by **FMT_SMR.1/PACE_EAC2PP**

FMT_MTD.1.1/PA_EAC2PP

The TSF shall restrict the ability to write[297] the card/chip security object(s) (SOC) and the document Security Object (SO_D)[298] to the Personalization Agent[299].

- **FMT_MTD.1/SK_PICC_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions: fulfilled by **FMT_SMF.1/EAC2PP**

FMT_SMR.1 Security roles fulfilled by **FMT_SMR.1/PACE_EAC2PP**

FMT_MTD.1.1/SK_PICC_EAC2PP

The TSF shall restrict the ability to create, load[300] the Chip Authentication private key(s) (SK_{PICC}) and the Restricted Identification Private Key(s)[301] to the personalization agent [302].

Application note 44: The formulation *Chip Authentication Private Key(s)* MUST be interpreted here to include the static keys of CA3 (i.e. $SK_{ICC,1}$, $SK_{ICC,2}$) as well.

[294] [assignment: list of EAC2 terminal types]
[295] [assignment: the authorised identified roles]
[296] [assignment: the authorized identified roles]
[297] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[298] [assignment: *list of TSF data*]
[299] [assignment: *the authorized identified roles*]
[300] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[301] [assignment: *list of TSF data*]
[302] [assignment: the authorized identified roles]

- **FMT_MTD.1/KEY_READ_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions fulfilled by **FMT_SMF.1/EAC2PP**

FMT_SMR.1 Security roles fulfilled by **FMT_SMR.1/PACE_EAC2PP**

FMT_MTD.1.1/KEY_READ_EAC2PP

The TSF shall restrict the ability to read[303] the

1. PACE passwords,
2. Personalization Agent Keys,
3. the Chip Authentication private key(s) (SK_{PICC})
4. the Restricted Identification private key(s)[304]
5. none[305]

to none[306].

Application note 45: The formulation *Chip Authentication Private Key(s)* MUST be interpreted here to include the static keys of CA3 (i.e. $SK_{ICC,1}$, $SK_{ICC,2}$) as well.

- **FMT_MTD.1/Initialize_PIN_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions **fulfilled** by **FMT_SMF.1/EAC2PP**

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/PACE_EAC2PP**

FMT_MTD.1.1/Initialize_PIN_EAC2PP

The TSF shall restrict the ability to write[307] the initial PIN and PUK[308] to the personalization agent[309].

- **FMT_MTD.1/Change_PIN_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

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

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

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

[306] [assignment: *the authorized identified roles*]

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

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

[309] [assignment: *the authorized identified roles*]

FMT_SMF.1 Specification of management functions **fulfilled** by **FMT_SMF.1/EAC2PP**
FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/PACE_EAC2PP**

FMT_MTD.1.1/Change_PIN_EAC2PP

The TSF shall restrict the ability to change[310] the blocked PIN[311] to EAC2 terminal (AT) with effective authorization for PIN Management.[312]

- **FMT_MTD.1/Resume_PIN_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions **fulfilled** by **FMT_SMF.1/EAC2PP**

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/PACE_EAC2PP**

FMT_MTD.1.1/Resume_PIN_EAC2PP

The TSF shall restrict the ability to resume[313] the suspended PIN[314] to the electronic document holder[315].

- **FMT_MTD.1/Unblock_PIN_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions **fulfilled** by **FMT_SMF.1/EAC2PP**

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/PACE_EAC2PP**

FMT_MTD.1.1/Unblock_PIN_EAC2PP

The TSF shall restrict the ability to unblock[316] the blocked PIN[317] to

1. the electronic document holder (using the PUK for unblocking)
2. an EAC2 terminal of a type that has the terminal authorization level for PIN management[318].

---

[310] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[311] [assignment: *list of TSF data*]
[312] [assignment: *the authorized identified roles*]/ [assignment: the authorised identified roles that match the list of PIN changing rules conformant to [TR03110-2]]
[313] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[314] [assignment: *list of TSF data*]
[315] [assignment: *the authorized identified roles*]
[316] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[317] [assignment: *list of TSF data*]
[318] [assignment: *the authorized identified roles*]

- **FMT_MTD.1/Activate_PIN_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions **fulfilled** by **FMT_SMF.1/EAC2PP**

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/PACE_EAC2PP**

FMT_MTD.1.1/Activate_PIN_EAC2PP

The TSF shall restrict the ability to activate and deactivate[319] the PIN[320] to an EAC2 terminal of a type that has the terminal authorization level for PIN management [321].

- **FMT_MTD.3/EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FMT_MTD.1 Management of TSF data **fulfilled** by **FMT_MTD.1/CVCA_INI_EAC2PP**, **FMT_MTD.1/CVCA_UPD_EAC2PP**, **FMT_MTD.1/DATE_EAC2PP**

FMT_MTD.3.1/EAC2PP

The TSF shall ensure that only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication protocol 2 and the Access Control SFP[322].

Refinement: To determine if the certificate chain is valid, the TOE shall proceed the certificate validation according to [TR03110-3].

- **FMT_LIM.1/EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FMT_LIM.2 Limited availability: **fulfilled** by **FMT_LIM.2/EAC2PP**

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

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

[321] [assignment: *the authorized identified roles*]

[322] [assignment: list of TSF data]

FMT_LIM.1.1/EAC2PP

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. embedded software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks.[323] and
5. none[324].

Application note 46: The above SFR concerns the whole TOE, not just applications with EAC2-protected data.

- **FMT_LIM.2/EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FMT_LIM.1 Limited capabilities: **fulfilled** by **FMT_LIM.1/EAC2PP**

FMT_LIM.2.1/EAC2PP

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. embedded software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks.[325] and
5. none[326].

Application note 47: The above SFR concerns the whole TOE, not just applications with EAC2-protected data.

[323] [assignment: Limited capability and availability policy]
[324] [assignment: Limited capability and availability policy]
[325] [assignment: Limited capability and availability policy]
[326] [assignment: Limited capability and availability policy]

- **FMT_MTD.1/INI_ENA_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions: **fulfilled** by **FMT_SMF.1/EAC2PP**

FMT_SMR.1 Security roles: **fulfilled** by **FMT_SMR.1/PACE_EAC2PP**

FMT_MTD.1.1/INI_ENA_EAC2PP

The TSF shall restrict the ability to write[327] the Initialisation Data and Pre-personalisation Data[328] to the Manufacturer[329].

- **FMT_MTD.1/INI_DIS_EAC2PP**

Hierarchical to:

No other components.

Dependencies:

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

FMT_SMF.1/EAC2PP

FMT_SMR.1 Security roles: **fulfilled** by **FMT_SMR.1/PACE_EAC2PP**

FMT_MTD.1.1/INI_DIS_EAC2PP

The TSF shall restrict the ability to read out and to use[330] the Initialisation Data[331] to the Personalisation Agent[332].

The following SFRs are imported due to claiming [EAC1PP]. They mainly concern applications with EAC1-protected data.

- **FMT_SMF.1/EAC1PP**

Hierarchical to:

No other components.

Dependencies:

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

[328] [assignment: list of TSF data]

[329] [assignment: the authorised identified roles]

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

[331] [assignment: list of TSF data]

[332] [assignment: the authorised identified roles]

No dependencies.

FMT_SMF.1.1/Specification of Management Functions_EAC1PP

The TSF shall be capable of performing the following management functions:

1. Initialisation,
2. Pre-Personalisation,
3. Personalisation
4. Configuration,[333]

- **FMT_SMR.1/PACE_EAC1PP**

This SFR is combined with **FMT_SMR.1/PACE_EAC2PP** into FMT_SMR.1

- **FMT_LIM.1/EAC1PP**

This SFR is equivalent to FMT_LIM.1/EAC2PP, but listed here for the sake of completeness.

- **FMT_LIM.2/EAC1PP**

This SFR is equivalent to FMT_LIM.2/EAC2PP, but listed here for the sake of completeness.

- **FMT_MTD.1/INI_ENA_EAC1PP**

(equivalent to FDP_MTD.1/INI_ENA_EAC2PP, but listed here for the sake of completeness)

- **FMT_MTD.1/INI_DIS_EAC1PP**

(equivalent to FDP_MTD.1/INI_DIS_EAC2PP, but listed here for the sake of completeness)

- **FMT_MTD.1/CVCA_INI_EAC1PP**

Hierarchical to:

No other components.

Dependencies:

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

FMT_SMF.1/EAC1PP

FMT_SMR.1 Security roles: **fulfilled** by **FMT_SMR.1/PACE_EAC1PP**

FMT_MTD.1.1/CVCA_INI_EAC1PP Management of TSF data – Initialisation of CVCA Certificate and Current Date

The TSF shall restrict the ability to write[334] the

1. initial Country Verifying Certification Authority Public Key (PK_{CVCA}),

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

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

2. initial Country Verifying Certification Authority Certificate (C_{CVCA}),,
3. initial Current Date,
4. none[335]

to Personalisation Agent[336].

- **FMT_MTD.1/CVCA_UPD_EAC1PP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions: **fulfilled** by **FMT_SMF.1/EAC1PP**

FMT_SMR.1 Security roles: **fulfilled** by **FMT_SMR.1/PACE_EAC1PP**

FMT_MTD.1.1/CVCA_UPD_EAC1PP

The TSF shall restrict the ability to update[337] the

1. Country Verifying Certification Authority Public Key (PK_{CVCA}),
2. Country Verifying Certification Authority Certificate (C_{CVCA}) ,
3. none[338].

to Country Verifying Certification Authority[339].

- **FMT_MTD.1/DATE_EAC1PP**

This SFR is equivalent to **FMT_MTD.1/DATE_EAC2PP** . Note that FMT_MTD.1/DATE_EAC2PP generalizes the notion of Domestic Extended Inspection System to EAC1 terminals with appropriate authorization level. This does not violate strict conformance to [EAC1PP].

- **FMT_MTD.1/CAPK_EAC1PP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions **fulfilled** by **FMT_SMF.1/EAC1PP**

[335] [assignement. List of TSF data]

[336] [assignment: the authorised identified roles]

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

[338][assignment: list of TSF data]

[339] [assignment: the authorised identified roles]

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/PACE_EAC1PP**

FMT_MTD.1.1/CAPK_EAC1PP

The TSF shall restrict the ability to load [340] the Chip Authentication Private Key [341] to Personalisation Agent[342].

- **FMT_MTD.1/PA_EAC1PP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions: **fulfilled** by **FMT_SMF.1/UPD_MREDONPP**

FMT_SMR.1 Security roles: **fulfilled** by **FMT_SMR.1/PACE_EAC1PP**

FMT_MTD.1.1/PA_EAC1PP

The TSF shall restrict the ability to write[343] the Document Security Object (SO_D)[344] to the Personalisation Agent. [345]

Application note 48: By writing SO_D into the TOE, the Personalisation Agent confirms (on behalf of DS) the correctness and genuineness of all the personalisation data related. This consists of user- and TSF- data.

- **FMT_MTD.1/KEY_READ_EAC1PP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions **fulfilled** by **FMT_SMF.1/EAC1PP**

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/PACE_EAC1PP**

FMT_MTD.1.1/KEY_READ_EAC1PP

The TSF shall restrict the ability to read [346] the

1. PACE passwords ,
2. Chip Authentication Private Key,
3. Personalisation Agent Keys[347]

[340] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]/[selection:create, load]

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

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

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

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

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

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

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

to none [348].

- **FMT_MTD.3/EAC1PP**

Hierarchical to:

No other components.

Dependencies:

FMT_MTD.1 Management of TSF data **fulfilled** by
FMT_MTD.1/CVCA_INI_EAC1PP,
FMT_MTD.1/CVCA_INI_EAC2PP,
FMT_MTD.1/CVCA_UPD_EAC1PP and
FMT_MTD.1/CVCA_UPD_EAC2PP

FMT_MTD.3.1/EAC1PP

The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol v.1 and the Access Control [349].

Refinement: The certificate chain is valid if and only if

1. **the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,**
2. **the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,**
3. **the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE.**

The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.

[348] [assignment: the authorised identified roles]

[349] [assignment: list of TSF data]

Application note 49: The Terminal Authentication Version 1 is used for Extended Inspection System as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.

The following SFRs are imported due to claiming [SSCDPP]. They mostly concern the security management of an *eSign* application.

- **FMT_SMR.1/SSCDPP**

Hierarchical to:

No other components.

Dependencies:

FIA_UID.1 Timing of identification **fulfilled** by **FIA_UID.1/SSCDPP**.

FMT_SMR.1.1/SSCDPP

The TSF shall maintain the roles R.Admin and R.Sigy[350].

FMT_SMR.1.2/SSCDPP

The TSF shall be able to associate users with roles.

- **FMT_SMF.1/SSCDPP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FMT_SMF.1.1/SSCDPP

The TSF shall be capable of performing the following security management functions:

1. Creation and modification of RAD,
2. Enabling the signature-creation function,
3. Modification of the security attribute SCD/SVD management, SCD operational,
4. Change the default value of the security attribute SCD Identifier,
5. none[351].

- **FMT_MOF.1/SSCDPP**

Hierarchical to:

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

[351] [assignment: list of other security management functions to be provided by the TSF]

No other components.

Dependencies:

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/SSCDPP**.

FMT_SMF.1 Specification of Management Functions **fulfilled** by **FMT_SMF.1/EAC2PP**.

FMT_MOF.1.1/SSCDPP

The TSF shall restrict the ability to enable[352] the signature-creation function[353] to R.Sigy[354].

- **FMT_MSA.1/Admin_SSCDPP**

Hierarchical to:

No other components.

Dependencies:

[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control] **fulfilled** by **FDP_ACC.1/SCD/SVD_Generation_SSCDPP**

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/SSCDPP**

FMT_SMF.1 Specification of Management Functions **fulfilled** by **FMT_SMF.1/SSCDPP**

FMT_MSA.1.1/Admin_SSCDPP

The TSF shall enforce the SCD/SVD_Generation_SFP[355] to restrict the ability to modify[356] [357] the security attributes SCD / SVD management[358] to R.Admin[359].

- **FMT_MSA.1/Signatory_SSCDPP**

Hierarchical to:

No other components.

[352] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
[353] [assignment: *list of functions*]
[354] [assignment: *the authorised identified roles*]
[355] [assignment: *access control SFP(s), information flow control SFP(s)*]
[356] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[357] None [assignment:other operations]. This assignment has only been written as a footnote as it would have been confusing in the main text.
[358] [assignment: *list of security attributes*]
[359] [assignment: *the authorised identified roles*]

Dependencies:

[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control] **fulfilled** by **FDP_ACC.1/Signature-creation_SSCDPP**

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/SSCDPP**

FMT_SMF.1 Specification of Management Functions **fulfilled** by **FMT_SMF.1/SSCDPP**

FMT_MSA.1.1/ Signatory_SSCDPP

The TSF shall enforce the Signature-creation_SFP[360] to restrict the ability to modify[361] the security attributes SCD operational[362] to R.Sigy[363].

- **FMT_MSA.2/SSCDPP**

Hierarchical to:

No other components.

Dependencies:

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control] **fulfilled** by **FDP_ACC.1/SCD/SVD_Generation_SSCDPP**, **FDP_ACC.1/Signature-creation_SSCDPP**

FMT_MSA.1 Management of security attributes **fulfilled** by **FMT_MSA.1/Admin_SSCDPP**, **FMT_MSA.1/Signatory_SSCDPP**

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/SSCDPP**

FMT_MSA.2.1/SSCDPP

The TSF shall ensure that only secure values are accepted for SCD / SVD Management and SCD operational[364].

- **FMT_MSA.3/SSCDPP**

Hierarchical to:

No other components.

[360] [assignment: *access control SFP(s), information flow control SFP(s)*]
[361] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[362] [assignment: *list of security attributes*]
[363] [assignment: *the authorised identified roles*]
[364] [selection: *list of security attributes*]

Dependencies:

FMT_MSA.1 Management of security attributes **fulfilled** by **FMT_MSA.1/Admin_SSCDPP**, **FMT_MSA.1/Signatory_SSCDPP**

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/SSCDPP**

FMT_MSA.3.1/SSCDPP

The TSF shall enforce the SCD/SVD_Generation_SFP, SVD_Transfer_SFP and Signature-creation_SFP[365] to provide restrictive[366] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/SSCDPP

The TSF shall allow the R.Admin[367] to specify alternative initial values to override the default values when an object or information is created.

- **FMT_MSA.4/SSCDPP**

Hierarchical to:

No other components.

Dependencies:

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control] **fulfilled** by **FDP_ACC.1/SCD/SVD_Generation_SSCDPP**, **FDP_ACC.1/Signature-creation_SSCDPP**

FMT_MSA.4.1/SSCD **Security attribute value inheritance**

The TSF shall use the following rules to set the value of security attributes:

1. If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute “SCD operational of the SCD” shall be set to “no” as a single operation.
2. If S.Sigy successfully generates an SCD/SVD pair the security attribute “SCD operational of the SCD” shall be set to “yes” as a single operation. [368]

[365] [assignment: *access control SFP, information flow control SFP*]

[366] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

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

[368] [assignment: *rules for setting the values of security attributes*]

- **FMT_MTD.1/Admin_SSCDPP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/SSCDPP**

FMT_SMF.1 Specification of Management Functions **fulfilled** by **FMT_SMF.1/SSCDPP**

FMT_MTD.1.1/Admin_SSCDPP

The TSF shall restrict the ability to create[369] the RAD[370] to R.Admin[371].

- **FMT_MTD.1/Signatory_SSCDPP**

Hierarchical to:

No other components.

Dependencies:

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/SSCDPP**

FMT_SMF.1 Specification of Management Functions **fulfilled** by **FMT_SMF.1/SSCDPP**

FMT_MTD.1.1/Signatory_SSCDPP

The TSF shall restrict the ability to modify[372] [373]the RAD[374] to S.Sigy[375].

The following SFRs are defined here. The concern loading applications onto the IC during manufacturing and relate directly to OT.Cap_Avail_Loader.

- **FMT_LIM.1/Loader Limited Capabilities**

[369] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[370] [assignment: *list of TSF data*]
[371] [assignment: *the authorised identified roles*]
[372] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[373] None [assignment:other operations]. This assignment has only been written as a footnote as it would have been confusing in the main text.
[374] [assignment: *list of TSF data*]
[375] [assignment: *the authorised identified roles*]

Hierarchical to:

No other components

Dependencies:

FMT_LIM.2/Loader Limited availability **fulfilled** by **FMT_LIM.2/Loader**

FMT_LIM.1.1/Loader

The TSF shall be designed and implemented in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Loader functionality after blocking the TOE Loader for TOE Delivery to the end-customer does not allow stored user data to be disclosed or manipulated by unauthorized users.[376]

Application note 50: FMT_LIM.1/Loader supplements FMT_LIM.2/Loader allowing for non-overlapping loading of user data and protecting the TSF against misuses of the Loader for attacks against the TSF. The TOE Loader may allow for correction of already loaded user data before the assigned action e.g. before blocking the TOE Loader for TOE Delivery to the end-customer or any intermediate step on the life cycle of the Security IC or the smartcard.

- **FMT_LIM.2/Loader Limited Availability**

Hierarchical to:
No other components

Dependencies:

FMT_LIM.1/Loader Limited capabilities **fulfilled** by **FMT_LIM.1/Loader**

FMT_LIM.2.1/Loader
The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: The TSF prevents deploying the Loader functionality after blocking the TOE Loader for TOE Delivery to the end-customer.[377]
Application note 51: The Loader functionality relies on a secure boot loading procedure in a secure environment before TOE delivery to the assigned user and preventing to deploy the Loader of the Security IC after an assigned action, e.g. after blocking the Loader for TOE delivery to the end-user.

The following SFRs come from [MR.ED-ON-PP].

[376] [assignment: *Limited capability and availability policy*]

[377] [assignment: *Limited capability and availability policy*]

FMT_SMF.1/UPD_MREDONPP Specification of Management Functions including Updates

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FMT_SMF.1.1/UPD_MREDONPP

The TSF shall be capable of performing the following management functions:

1) Updating the TOE software with the mechanism specified in HUiF[378][379].

- **FMT_MTD.1/UPD_SK_PICC_MREDONPPManagement of TSF Data – Secret Update Keys**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions:**fulfilled** by **FMT_SMF.1/UPD_MREDONPP**

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/UPD_MREDONPP**

FMT_MTD.1.1/UPD_SK_PICC_MREDONPP

The TSF shall restrict the ability to l*oad* [380] the Secret Cryptographic Keys defined in HUiF[381] to the update key installation agent[382].

- **FMT_MTD.1/UPD_KEY_READ_MRENONPP Management of TSF data – Secret Update Keys**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions **fulfilled** by **FMT_SMF.1/UPD_MREDONPP**

FMT_SMR.1 Security roles **fulfilled** by **FMT_SMR.1/UPD_MREDONPP**

FMT_MTD.1.1/UPD_KEY_READ_MREDONPP

The TSF shall restrict the ability to read[383] the

1) Secret Cryptographic Update Keys defined in HUiF [384]

[378] [assignment: *list of technical specification(s) defining an update mechanism*]

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

[380] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] / [selection: *create, load*]

[381] [assignment: *list of TSF data*] / [selection: *list of, or reference specifying the Secret Cryptographic Update Keys required for the update procedure*]

[382] [assignment: *the authorized identified roles*]

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

[384] [assignment: list of or reference specifying the Secret Cryptographic Update Keys required for the update procedure]

2) none[385]
to none[386].

- **FMT_SMR.1/UPD_MREDONPP Security roles**

Hierarchical to:

No other components.

Dependencies:

FIA_UID.1 Timing of identification:**fulfilled** by **FIA_UID.1/UPD_MREDONPP**

FMT_SMR.1.1/UPD_MREDONPP

The TSF shall maintain the roles

1) terminal,
2) update terminal
3) update key installation agent
4) Encryption agent
5) Signature1 Agent
6) Signature2 Agent[387]

FMT_SMR.1.2/UPD

The TSF shall be able to associate users with roles.

6.1.7 Class FPT

The following security functional requirements are imported from [EAC2PP], and address the protection against forced illicit information leakage, including physical manipulation.

- **FPT_EMS.1/EAC2PP TOE Emanation**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPT_EMS.1.1/EAC2PP

The TOE shall not emit information about IC power consumption, electromagnetic radiation and command execution time[388]in excess of non-useful information[389] enabling access to

1. **the** session keys (PACE-KMAC, PACE-KEnc), **(CA-KMAC, CA-KEnc, both CA2 and CA3)** ,
2. the ephemeral private key ephem - SK_{PICC} - PACE,
3. the Chip Authentication private keys (SK_{PICC}), **both CA2 and CA3,**

[385] [assignment: *list of TSF data*]
[386] [assignment: *the authorized identified roles*]
[387] [assignment: *the authorized identified roles*]
[388] [*assignment: types of emissions*]
[389] [assignment: *specified limits*]

4. the PIN, PUK,
5. the additional Chip Authentication 3 private sector keys ($SK_{ICC,1}$ and $SK_{ICC,2}$) [390]
6. none[391]

and

7. the Restricted Identification private key(s) SK_{ID} ,
8. none[392].

FPT_EMS.1.2/EAC2PP

The TSF shall ensure any users are unable to use the following interface electronic document 's contactless **/contact-based interface** and circuit contacts to gain access to

1. **the** session keys (PACE-K_{MAC}, PACE-K_{ENC}), **(CA-K_{MAC}, CA-K_{ENC}, both CA2 and CA3)**
2. the ephemeral private key ephem - SK_{PICC} - PACE,
3. the Chip Authentication private key(s) (SK_{PICC}), **both CA2 and CA3,**
4. the PIN, PUK,
5. the session keys (PACE-K_{MAC}, PACE-K_{ENC}), (CA-K_{MAC}, CA-K_{ENC})
6. the additional Chip Authentication 3 private sector keys ($SK_{ICC,1}$ and $SK_{ICC,2}$)[393]
7. none[394]

and

8. the Restricted Identification private key(s) SK_{ID},
9. none[395].

Application note 52: Note that related to *Application Note 6*, the PIN in the above SFR refers here to both the PIN for an eID application, and also the PIN for an eSign application, if they exist on card.
The above SFR is refined from [EAC2PP] by adding all relevant key material from Chip Authentication 3 in addition to the key material from Chip Authentication 2, as well as the additional assignment to cover the private sector keys. Thus the set of keys that need to be protected is a superset of the ones of the SFR from [EAC2PP]. Hence, the requirement is more stricter than the one from [EAC2PP], and the refinement operation is justified.
A refinement is used here to ensure that emissions via contact-based interfaces must not be observable as well. This extends the scope of

[390] [assignment: *list of types of TSF data*]
[391] [assignment: *list of types of TSF data*]
[392] [assignment: *list of types of user data*]
[393] [assignment: *list of types of TSF data*]
[394] [assignment: *list of types of TSF data*]
[395] [assignment: *list of types of user data]*

emission analysis by creating a stricter requirement. Hence, the refinement is justified.

- **FPT_FLS.1/EAC2PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPT_FLS.1.1/EAC2PP

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[396].

- **FPT_TST.1/EAC2PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPT_TST.1.1/EAC2PP

The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation, at the condition*[397] Reset of the TOE[398] to demonstrate the correct operation of the TSF[399].

FPT_TST.1.2/EAC2PP

The TSF shall provide authorised users with the capability to verify the integrity of the TSF data[400].

FPT_TST.1.3/EAC2PP

The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code[401].

[396] [assignment: list of types of (further) failures in the TSF]

[397] [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions]

[398] [assignment: conditions under which self test should occur]

[399] [selection: [assignment: parts of TSF], the TSF]

[400] [selection: [assignment: parts of TSF], TSF data]

[401] [selection: *[assignment: parts of TSF], TSF*]

- **FPT_PHP.3/EAC2PP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPT_PHP.3.1/EAC2PP

The TSF shall resist physical manipulation and physical probing[402] to the TSF[403] by responding automatically such that the SFRs are always enforced.

The following SFRs are imported due to claiming [EAC1PP]. They mostly concern the protection of security functionality related to EAC1-protected data.

- **FPT_TST.1/EAC1PP**(equivalent to FPT_TST.1/EAC2PP, but listed here for the sake of completeness)
- **FPT_FLS.1/EAC1PP**(equivalent to FPT_FLS.1/EAC2PP, but listed here for the sake of completeness)
- **FPT_PHP.3/EAC1PP**(equivalent to FPT_PHP.3/EAC2PP, but listed here for the sake of completeness)

- **FPT_EMS.1/EAC1PP Emanation**

Hierarchical to:

No other components

Dependencies:

No dependencies.

FPT_EMS.1.1/EAC1PP

The TOE shall not emit information about IC power consumption,electromagnetic radiation and command execution time [404] in excess of non useful information [405] enabling access to

1. Chip Authentication **(Version 1)** Session Keys
2. PACE session Keys (PACE- K_{MAC}, PACE- K_{ENC}),
3. the ephemeral private key ephem SK_{PICC} -PACE,
4. the ephemeral private key $SK_{Map,PICC}$ -PACE-CAM[406]
5. none[407],
6. Personalization Agent Key(s),
7. Chip Authentication **(Version 1)** Private Key[408] and

[402] [assignment: physical tampering scenarios]
[403] [assignment: list of TSF devices/elements]
[404] [assignment: types of emissions]
[405] [assignment: specified limits]
[406] [assignment: list of types of TSF data]
[407] [assignment: list of types of TSF data]
[408] [assignment: list of types of TSF data]

8. none[409]

FPT_EMS.1.2/EAC1PP

The TSF shall ensure any users are unable to use the following interface smart card circuit contacts to gain access to

1. Chip Authentication **(Version 1)** Session Keys
2. PACE Session Keys (PACE- K_{MAC}, PACE- K_{ENC}),
3. the ephemeral private key ephem SK_{PICC} -PACE,
4. the ephemeral private key $SK_{Map,PICC}$-PACE-CAM[410]
5. none[411],
6. Personalization Agent Key(s),
7. Chip Authentication **(Version 1)** Private Key[412]
8. none[413]

Application note 53: This SFR covers the definition of FPT_EMS.1 in [EAC1PP] and extends it by 4. of FPT_EMS.1.1 and FPT_EMS.1.2. Also, 1. and 7. of both FPT_EMS.1.1 and FPT_EMS.1.2 are slightly refined in order not to confuse Chip Authentication 1 with Chip Authentication 2 or Chip Authentication 3. Note that FPT_EMS.1 in [EAC1PP] is solely concerned with Chip Authentication 1, but since it was the first version of the protocol at the time, it was simply called 'Chip Authentication' back then.W.r.t. PACE-CAM, note the significance of protecting SKMap,PICC-PACE-CAM: Whereas when running PACE and CA1 separately, gaining knowledge of the ephemeral key SK_{PICC} -PACE enables the attacker to decrypt the current PACE session, an attacker that gains knowledge of the ephemeral key SKMap,PICC-PACE-CAM can not only decrypt the session but also easily reveal the static secret chip authentication key SK_{PICC}: Let ° denote the group operation (i.e. addition or multiplication), and let i(x) denote the inverse of x. Since the chip sends CAPICC = SKMap,PICC-PACE-CAM ° i(SK_{PICC}) to the terminal, a malicious attacker that gains knowledge of SKMap,PICC-PACE-CAM can reveal SK_{PICC} by computing SK_{PICC} = i(CAPICC) ° SKMap,PICC-PACE-CAM.

The following SFRs are imported due to claiming [SSCDPP]. They mostly concern the protection of security functionality related to eSign application (if available).

- **FPT_EMS.1/SSCDPP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPT_EMS.1.1/SSCDPP

[409] [assignment: list of types of user data]
[410] [assignment: list of types of TSF data]
[411] [assignment: list of types of TSF data],
[412] [assignment: list of types of TSF data]
[413] [assignment: list of types of user data]

The TOE shall not emit information about IC power consumption, electromagnetic radiation and command execution time[414] in excess of non useful information[415] enabling access to RAD[416] and SCD[417]

FPT_EMS.1.2/SSCDPP

The TSF shall ensure any user are unable to use the following interface card's contactless interface and circuit contacts to gain access to RAD[418] and SCD[419].

- **FPT_FLS.1/SSCDPP** (subsumed by FPT_FLS.1/EAC2PP)
- **FPT_PHP.1/SSCDPP**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPT_PHP.1.1/SSCDPP

The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2/SSCDPP

The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

- **FPT_PHP.3/SSCDPP** (subsumed by **FPT_PHP.3/EAC2PP**)
- **FPT_TST.1/SSCDPP** (subsumed by **FPT_TST.1/EAC2PP**)

The following SFRs come from [SSCDPP].

- **FPT_EMS.1/UPD_MREDONPP** **TOE Emanation**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPT_EMS.1.1/UPD_MREDONPP

[414] [assignment: types of emissions]
[415] [assignment: specified limits]
[416] [assignment: list of types of (further) TSF data]
[417] [assignment: list of types of (further) user data
[418] [assignment: list of types of (further) TSF data]
[419] [assignment: list of types of (further) user data

The TOE shall not emit information about IC power consumption, electromagnetic radiation and command execution time [420] in excess of non useful information [421] enabling access to the Secret Cryptographic Update Keys used for the update mechanism and other types of TSF data defined in HUiF [422] and none[423].

FPT_EMS.1.2/UPD_MREDONPP
The TSF shall ensure any users[424] are unable to use the following interface electronic document 's contactless/contact-based interface and circuit contacts[425] to gain access to the Secret Cryptographic Update Keys used for the update mechanism and other types of TSF data defined in HUiF [426] none[427].

Application Note 54: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE, originate from internal operation of the TOE, or be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. Examples of measurable phenomena include, but are not limited to variations in power consumption, timing of signals, and electromagnetic radiation due to internal operations or data transmissions. Note that while the security functionality described in FPT_EMS.1 should be taken into account during development of the TOE, associated tests must be carried out as part of the evaluation, and not/not only during product development.FPT_EMS.1/UPD is an iteration of the definition of FPT_EMS.1 (defined as an extended component in [MR.ED2.0]). That base PP also contains several other iterations of FPT_EMS.1, such as FPT_EMS.1/EAC1PP, and FPT_EMS.1/EAC2PP. These multiple definitions do not contradict, since one of course must apply a logical 'AND' w.r.t. to all data defined in all FPT_EMS.1/*, i.e. none of any data defined FPT_EMS.1/* must be observable or accessible according to FPT_EMS.1.1 and FPT_EMS.1.2.

---

[420] [assignment: *types of emissions*]
[421] [assignment: *specified limits*]
[422] [assignment: *list of types of TSF data*]/ [assignment: list of or reference specifying the Secret Cryptographic Update Keys used for the update mechanism and other types of TSF data]
[423] [assignment: *list of types of user data*]
[424] [assignment: *type of users*]
[425] [assignment: *type of connection*]
[426] [assignment: *list of types of TSF data*]/ [assignment: list of or reference specifying the Secret Cryptographic Update Keys used for the update mechanism and other types of TSF data]
[427] [assignment: *list of types of user data*]

- **FPT_FLS.1/UPD_MREDONPP Failure with Preservation of Secure State (Failed Update)**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FMT_FLS.1.1/UPD_MREDONPP

The TSF shall preserve a secure state when the following types of failures occur:

1) Failure during a transmission of the update package data file
2) Failure detected by TSF according to FPT_TST.1
3) Failure detected after a failed update[428]
4) none[429].

Application Note 55: The secure state after a failed update should be achieved by reverting to the previous TOE software version. Nevertheless this capability will have limits, since the atomicity of the software update mechanism can technically only be achieved up to a certain extent.

- **FPT_TST.1/UPD_MREDONPP TSF Testing (after Installation of an Update)**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FMT_TST.1.1/ UPD_MREDONPP

The TSF shall run a suite of self tests *at the Condition Reset of the TOE*[430]to demonstrate the correct operation of the TSF[431].

FPT_TST.1.2/ UPD_MREDONPP

The TSF shall provide authorized users with the capability to verify the integrity of the TSF data[432].

FPT_TST.1.3/UPD_MREDONPP

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

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

[430] [selection: *during initial start-up, periodically during normal operation, after a software update, at the request of the authorized user, at the conditions* [assignment: *conditions under which self test should occur*]]

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

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

The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code[433].

6.2 Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE, its development and operating environment are to choose as the predefined assurance package EAL4 augmented by the following components:

- ALC_DVS.2 (Sufficiency of security measures),
- ATE_DPT.2 (Testing: security enforcing modules) and
- AVA_VAN.5 (Advanced methodical vulnerability analysis).

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

The following table provides an overview for the coverage of the security functional requirements, and also gives evidence for sufficiency and necessity of the chosen SFRs.

[433] [selection: *[assignment: parts of TSF], TSF*]

	OT.Chip_Auth_Proof (EAC1PP)	OT.Chip_Auth_Proof_PACE_CAM	OT.Sens_Data_Conf (EAC1PP)	OT.AC_Pers_EAC2	OT.CA3	OT.Sens_Data_EAC2	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Identification*	*OT.AC_Pers*	*OT.Prot_Inf_Leak*	OT.Non_Interfere	OT.SCD/SVD_Gen (SSCDPP)	OT.Sigy_SigF (SSCDPP)	OT.Cap_Avail_Loader	OT.RI_EAC2
Class FCS																	
FCS_CKM.1/CA3					x	X	x	x	x								
FCS_COP.1/CA3					x	X	x	x	x								
FCS_CKM.1/CAM		x					x	x	x								
FCS_COP.1/CAM		x					x	x	x								
Class FIA																	
FIA_API.1/CA3					x	X	x	x	x								x
FIA_UAU.5/PACE_EAC2PP					x	X	x	x	x								x
FIA_UAU.6/CA3					x	X	x	x	x								
FIA_UID.1/PACE_EAC1PP		x	x				x	x	x		x						
FIA_UAU.5/PACE_EAC1PP		x	x				x	x	x		x						
FIA_API.1/PACE_CAM		x					x	x	x								
FIA_UAU.1/SSCDPP														x	x		
Class FDP																	
FDP_ACF.1/TRM			x	x		X	x		x		x		x				
Class FMT																	
FMT_SMR.1	x			x		X	x	x	x	x	x		x				
FMT_LIM.1/Loader																x	
FMT_LIM.2/Loader																x	
Class FTP																	
FTP_ITC.1/CA3					x		x	x	x								
Class FPT																	
FPT_EMS.1/EAC1PP											x	x	x				
FPT_EMS.1/EAC2PP				x								x	x				
FPT_EMS.1/SSCDPP													x				

Table 5 Coverage of Security Objectives for the TOE by SFRs

According to [CC1], tracing between SFRs and security objectives must ensure that 1) each SFR traces back to at least one security objective, and 2) that each security objective for the TOE has at least one SFR tracing to it. This is illustrated for

1. SFRs that have been newly added or refined within this ST by checking the *rows* of Table 4, and for SFRs that are merely iterated

or simply included due to claims of other protection profiles by looking up the rationale of that PP

2. for newly introduced security objectives in this ST by checking the non-cursive *columns* of Table 4, and for the other security objectives by looking up the rationale of that PP.

In other words, in Table 4, we list only:

- SFRs that have been newly added or refined within this ST. Mere iterations or simple inclusions due to claims of other protection profiles are not listed however. For their coverage we refer to the respective claimed PP.
- Security objectives that are newly introduced in this ST, and their related SFRs.
- Security objectives for the TOE that are affected by the above newly added or refined SFRs.

Analogously, we limit our justification to the above SFRs and security objectives. For other security objectives, and for the justification of security objectives w.r.t. SFRs that are included or iterated from claimed protection profiles, we refer to the detailed rationales in [EAC1PP], [EAC2PP] and [SSCDPP].

OT.Chip_Auth_Proof_PACE_CAM is a newly introduced security objective that aims to ensure the authenticity of the electronic document's chip by the PACE-CAM protocol, in particular in the context of an ePassport application. This is supported by **FCS_CKM.1/CAM** for cryptographic key-generation, and **FIA_API.1/PACE_CAM** and **FCS_COP.1/CAM** for the implementation itself, as well as **FIA_UID.1/PACE_EAC1PP** and **FIA_UAU.5/PACE_EAC1PP**, the latter supporting the PACE protocol.

OT.CA3 is a newly introduced security objective that aims to ensure the authenticity of the electronic document's chip while at the same time providing providing a very high level of protection against tracing. This is achieved by the Chip Authentication Version 3 (CA3) protocol. The security objective is supported by **FCS_CKM.1/CA3** for cryptographic key generation during CA3, and **FIA_API.1/CA3, FCS_COP.1/CA3** and **FIA_UAU.6/CA3** for the implementation of CA3 itself, **FTP_ITC.1/CA3** for secure communication with the TOE, as well as the refined SFRs **FIA_UAU.5/PACE_EAC2PP**, **FIA_UID.1/PACE_EAC1PP**, and **FIA_UAU.5/PACE_EAC1PP**.

The new **SFR FTP_ITC.1/CA3** provides an inter-trusted channel with the TOE using the CA3 protocol. The CA3 protocol is used to derive a shared secret, which itself provides encryption and integrity protection of the channel. Hence, the security objectives **OT.Data_Confidentiality** and **OT_Data_Integrity** are also supported by this SFR. The CA3 protocol itself is also used to authenticate the TOE to the communicating

party. Therefore, **OT.Data_Authenticity** is supported by this SFR as well.

Aside the new SFRs mainly concerned with the above new security objectives, we discuss the remaining new and refined SFRs:

FIA_UAU.1/SSCDPP is refined here in a way that the TOE supports additionally EAC2 based access control w.r.t. SSCD-related user data. This does not affect the discussion of the rationale of [SSCDPP].
FDP_ACF.1/TRM unifies the access control SFPs of **FDP_ACF.1/TRM_EAC2PP** and **FDP_ACF.1/TRM_EAC1PP**. Both access control SFPs however are maintained w.r.t. sensitive EAC1-protected data and EAC2-protected data. Thus the discussion of the rationale of [EAC1PP] and [EAC2PP] remains unaffected.

FMT_SMR.1/EAC1PP and **FMT_SMR.1/EAC2PP** have been unified to **FMT_SMR.1** by adding additional roles. For all security objectives affected, FMT_SMR.1 supports related roles analogously as in the discussion of the rationales of [EAC1PP] and [EAC2PP].

The security objective **OT.Cap_Avail_Loader** is directly covered by the SFRs **FMT_LIM.1/Loader** and **FMT_LIM.2/Loader**, which limits the availability of the loader, as required by the objective.

FPT_EMS.1/EAC1PP and **FPT_EMS.1/EAC2PP** together define all protected data. Since all previous data are included, the discussion of the rationales of [EAC1PP] and [EAC2PP] is not affected.

The objective **OT.Non_Interfere** aims to ensure that no security related interferences between the implementations of the different access control mechanisms exist that allow unauthorized access of user or TSF-Data. This objective is fulfilled by enforcing the access control SFPs, in particular **FDP_ACF.1/TRM** in connection with **FDP_ACC.1/TRM_EAC1PP.** Related roles are supported by **FMT_SMR.1**. Interferences that are observable by emissions from the TOE are prevented due to **FPT_EMS.1/EAC1PP, FPT_EMS.1/EAC2PP, and FPT_EMS.1/SSCDPP**, where the set union of all defined data covers all relevant data.

6.3.1.1 Security Functional Requirements Rationale for the Security Functional Requirements coming from [MR.ED-ON-PP]

The following table provides an overview for the coverage of the security functional requirements, and also gives evidence for sufficiency and necessity of the chosen SFRs.
The SFRs FCS_COP.1/UPD_ITC, FCS_CKM.1/UPD_ITC, FCS_COP.1/UPD_DEC, FCS_CKM.1/UPD_DEC, FCS_COP.1/UPD_INT, FCS_CKM.1/UPD_INT, FCS_COP.1/UPD_SIG, FCS_CKM.4/UPD are concerned with cryptographic operations and key

generation. They support the objectives OT.Update_Mechanismand OT.Enc_Sign_Update.
FIA_AFL.1/UPD, FIA_UID.1/UPD, FIA_UAU.1/UPD are concerned with identification and authentication towards the TOE. They concern the update mechanism and hence OT.Update_Mechanism, and OT.Update_Terminal_Auth.
FDP_ACC.1/UPD, FDP_ACF.1/UPD, FDP_IFC.1/UPD, FDP_IFF.1/UPD support OT.Update_Mechanism and OT.Update_Terminal_Auth.
FDP_RIP.1/UPD supports OT.Update_Mechanism.

FAU_SAS.1/UPD supports OT.Update_Mechanism and OT.Attack_Detection w.r.t. logging.
FMT_SMF.1/UPD, FMT_MTD.1/UPD_SK_PICC, FMT_MTD.1/UPD_KEY_READ, and FMT_SMR.1/UPD are concerned with management functions and data. FMT_SMF.1/UPD supports OT.Update_Mechanism, FMT_MTD.1/UPD_SK_PICC and FMT_MTD.1/UPD_KEY_READ support OT.Enc_Sign_Update, OT.Update_Terminal_Auth and OT.Key_Secrecy, and FMT_SMR.1/UPD supports OT.Enc_Sign_Update, OT.Update_Terminal_Auth.

	OT.Update_Mechanism	OT.Enc_Sign_Update	OT.Update_Terminal_Auth	OT.Attack_Detection	OT.Key_Secrecy
Class FCS					
FCS_COP.1/UPD_ITC_MREDONPP	x	x			
FCS_CKM.1/UPD_ITC_MREDONPP	x	x			
FCS_COP.1/UPD_DEC_MREDONPP	x	x			
FCS_CKM.1/UPD_DEC_MREDONPP	x	x			
FCS_COP.1/UPD_INT_MREDONPP	x	x			
FCS_CKM.1/UPD_INT_MREDONPP	x	x			
FCS_COP.1/UPD_SIG_MREDONPP	x	x			
FCS_CKM.4/UPD_MREDONPP	x	x			
Class FIA					
FIA_AFL.1/UPD_MREDONPP	x		x		
FIA_UID.1/UPD_MREDONPP	x		x		
FIA_UAU.1/UPD_MREDONPP	x		x		
Class FDP					
FDP_ACC.1/UPD_MREDONPP	x		x		
FDP_ACF.1/UPD_MREDONPP	x		x		
FDP_IFC.1/UPD_MREDONPP	x		x		
FDP_IFF.1/UPD_MREDONPP	x		x		
FDP_RIP.1/UPD_MREDONPP	x				
Class FAU					
FAU_SAS.1/UPD_MREDONPP	x			x	
Class FMT					
FMT_SMF.1/UPD_MREDONPP	x				
FMT_MTD.1/UPD_SK_PICC_MREDONPP		x	x		x
FMT_MTD.1/UPD_KEY_READ_MREDONPP		x	x		x
FMT_SMR.1/UPD_MREDONPP		x	x		
Class FPT					
FPT_EMS.1/UPD_MREDONPP					x
FPT_FLS.1/UPD_MREDONPP				x	
FPT_TST.1/UPD_MREDONPP				x	
Class FTP					

FTP_ITC.1/UPD_MREDONPP	x		x		

Table 6 Coverage of [MR.ED-ON-PP] Security Objectives for the TOE by the SFRs

6.3.2 Rationale for SFR's Dependencies

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 dependency analysis has directly been made within the description of each SFR in Section 6.1 above. All dependencies being expected by [CC2] and by extended components definition in Chapter 5 are either fulfilled, or their non-fulfillment is justified.

6.3.3 Security Assurance Requirements Rationale

The current assurance package was chosen based on the predefined assurance package EAL4. This package permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level, at which it is likely to retrofit to an existing product line in an economically feasible way. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the electronic document's development and manufacturing, especially for the secure handling of sensitive material.

The selection of the component ATE_DPT.2 provides a higher assurance than the predefined EAL4 package due to requiring the functional testing of SFR-enforcing modules.

The selection of the component AVA_VAN.5 provides a higher assurance than the predefined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 3, entry 'Attacker'). This decision represents a part of the conscious security policy for the electronic document required by the electronic document issuer and reflected by [MR.ED2.0].

The set of assurance requirements being part of EAL4 fulfills all dependencies a priori. The augmentation of EAL4 chosen comprises the following assurance components: ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. For these additional assurance component, all dependencies are met or exceeded in the EAL4 assurance package. Below we list only those assurance requirements that are additional to EAL4.

ALC_DVS.2
Dependencies: None
ATE_DPT.2
Dependencies: ADV_ARC.1, ADV_TDS.3, ATE_FUN.1fulfilled by ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
AVA_VAN.5
Dependencies:ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1fulfilled by ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.2

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) are internally consistent. The analysis of the TOE´s security requirements with regard to their mutual support and internal consistency demonstrates:

The dependency analysis 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 justified.

All subjects and objects addressed by more than one SFR are also treated in a consistent way: the SFRs impacting them do not require any contradictory property or behavior of these ‘shared’ items.

The assurance package EAL4 is a predefined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in Section 6.3.3 shows that the assurance requirements are internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements can only arise due to functional-assurance dependencies not being met. As shown in Section 6.3.2 and Section 6.3.3,the chosen assurance components are adequate for the functionality of the TOE. Hence, there are no inconsistencies between the goals of these two groups of security requirements.

6.4 Statement of Compatibility

This is a statement of compatibility between this Composite Security Target (Composite-ST) and the Platform Security Target (Platform-ST) of the SLC52GDA448 [HWST]. This statement is compliant to the requirements of [COMPEVAL].

6.4.1 Classification of Platform TSFs

A classification of TSFs of the Platform-ST has been made. Each TSF has been classified as ‘relevant’ or ‘not relevant’ for the Composite-ST.

TOE Security Functionality	Relevant	Not relevant
SF_DPM: Device Phase Management	X	
SF_PS: Protection against Snooping	X	
SF_PMA: Protection against Modifying Attacks	X	
SF_PLA: Protection against Logical Attacks	X	
SF_CS: Cryptographic Support	X	

Table 7: Classification of Platform-TSFs

All listed TSFs of the Platform-ST are relevant for the Composite-ST.

6.4.2 Matching statement

The TOE relies on fulfillment of the following implicit assumptions on the IC:

- Certified Infineon Microcontroller SLC52GDA448; the optional RSA2048/4096 libraries are not used by this TOE,
- Hybrid Random Number Generation with PTG.2 classification according to [AIS31],
- Cryptographic support based on asymmetric and symmetric key algorithms (EC-DSA, AES) with 192 -512 bit asymmetric key length and 128 - 256 bit symmetric cryptographic key length.

The rationale of the Platform-ST has been used to identify the relevant SFRs, TOE objectives, threats and OSPs. All SFRs, objectives for the TOEs, but also all objectives for the TOE-environment, all threats and OSPs of the Platform-ST have been used for the following analysis.

6.4.2.1 **TOE Security Environment**

6.4.2.1.1 Threats and OSPs

(see chapters 3.2 and 3.3)

None of the OSPs of the Composite-ST are applicable to the IC and therefore not mapable for the Platform-ST.

The augmented organizational security policy P.Add-Functions of the Platform-ST deals with additional specific security components like the AES encryption and decryption and could therefore be mapped to OT.Prot_Inf_Leak and OT.Prot_Phys-Tamper of the Composite-ST.

The organizational security policy P.Process-TOE of the Platform-ST deals with an accurate identification of the TOE during the first phases of its lifecycle up to the TOE delivery in phase 3 (test mode) of the Plattform TOE. Later on each variant of the TOE has to protect itself. Therefore P.Process-TOE of the Platform-ST is not mapable to the OSPs and the threats of the Composite-ST.

The following threats of this Composite-ST are directly related to IC functionality:

- T.Phys-Tamper
- T.Malfunction
- T.Abuse-Func
- T.Information_Leakage
- T.Forgery

These threats will be mapped to the following Platform-ST threats:

- T.Leak-Inherent
- T.Phys_Probing
- T.Malfunction
- T.Phys_Manipulation
- T.Leak-Forced
- T.Abuse-Func
- T.RND
- T.Mem-Access

The following table shows the mapping of the threats.

Platform-ST		T.Leak-Inherent	T.Phys_Probing	T.Phys_Manipulation	T.Malfunction	T.Leak-Forced	T.Abuse-Func	T.RND	T.Mem-Access
Composite-ST	T.Phys-Tamper	X	X	X	X	X		X	
	T.Malfunction				X				
	T.Abuse-Func						X		X
	T.Information_Leakage	X	X	X	X	X	X		
	T.Forgery			X	X				

Table 8 Mapping of threats

T. Phys-Tamper matches to T.Leak-Inherent, T.Phys_Probing, T.Malfunction, T.Phys-Manipulation, T.Leak-Forced and T.RND as physical TOE interfaces like emanations, probing, environmental stress and tampering are used to exploit vulnerabilities.

T.Abuse-Func matches to T.Mem-Access as security violations either accidentally or deliberately could access restricted data (which may include code) or privilege levels.

T.Information_Leakage matches to T.Leak-Inherent, T.Phys_Probing, T.Malfunction, T.Phys-Manipulation, T.Leak-Forced and T.Abuse-Func as physical TOE interfaces like emanations, probing, environmental stress and tampering could be used to exploit exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data.

T.Forgery matches to T.Phys_Manipulation and T.Malfunction because if an attacker fraudulently alters the User Data or/and TSF-data stored on the ID_Card or/and exchanged between the TOE and the Service Provider then the listed threats of the Platform-ST could be relevant.

6.4.2.1.2 Assumptions

(see chapter 3.4)

The assumptions from this ST (A.CGA, A.SCA, A.Auth_PKI, A.Insp_Sys and A.Passive_Auth) make no assumption on the Platform, but to the environment of the TOE.

The assumptions from the Platform-ST are as follows:

Assumption	Classification of assumptions	Mapping to Security Objectives of this Composite-ST
A.Process-Sec-IC [HWST]	not relevant	n/a
A.Resp-Appl [HWST]	relevant	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper, OT.SCD/SVD_Auth_Gen, OT.SCD_SVD_Corresp, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE. All of the above listed Security Objectives of this Composite TOE aim to protect the user data, especially SCD, SVD, DTBS and RAD.
A.Key-Function	relevant	OT.Prot_Inf_Leak and OT.EMSEC_Design require that Key-dependent functions are implemented in a way that they are not susceptible to leakage attacks.

Table 9 Mapping of assumptions

There is **no conflict** between **security environments** of this Composite-ST and the Platform-ST [HWST].

6.4.2.2 Security objectives

This Composite-ST has security objectives which are related to the Platform-ST.

These are:

- OT.SCD_Secrecy
- OT.SCD_Unique
- OT.Tamper_ID
- OT.Tamper_Resistance
- OT.Prot_Abuse-Func
- OT.Prot_Inf_Leak
- OT.Prot_Phys-Tamper
- OT.Identification
- OT.Prot_Malfunction
- OT.Cap_Avail_Loader, OE.Lim_Block_Loader
- OT.Data_Confidentiality

The following Platform-objectives could be mapped to Composite-objectives:

- O.RND
- O.Phys-Probing
- O.Malfunction
- O.Phys-Manipulation
- O.Abuse-Func
- O.Leak-Forced
- O.Leak-Inherent
- O.Identification
- O.Cap_Avail_Loader, O.Authentication, O.Ctrl_Auth_loader, O.Prot_TSF_Confidentiality
- O.AES
- O.TDES

These could be mapped to the Composite-objectives as seen in the following table.

Platform-ST		O.RND	O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Abuse-Func	O.Leak-Forced	O.Leak-Inherent	O.Identification	O.Cap_Avail_Loader, O.Authentication, O.Ctrl_Auth_Loader, O.Prot_TSF_Confidentiality	O.AES	O.TDES
Composite-ST	OT.SCD_Secrecy	X										
	OT.SCD_Unique	X										
	OT.Tamper_ID		X	X	X							
	OT.Tamper_Resistance		X	X	X							
	OT.Prot_Abuse-Func					X						
	OT.Prot_Inf_Leak						X	X				
	OT.Prot_Phys-Tamper		X	X	X							
	OT.Identification								X			
	OT.Prot_Malfunction			X								
	OT.Cap_Avail_Loader, OE.Lim_Block_Loader									X		
	OT.Data_Confidentiality										X	X

Table 10 Mapping of objectives

O.Cap_Avail_Loader, O.Authentication, O.Ctrl_Auth_Loader and O.Prot_TSF_Confidentiality : The ST Flash Loader is used to load the encrypted initialization image into the flash memory of the chips during Initialization (after Phase 4) and Composite Product Integration (in Phase 5). The usage of the Loader is addressed in [AGD_PRE] and by OE.Lim_Block_Loader and OT.Cap_Avail_Loader. In User configuration (Step 7), the Loader capability is not accessible by the Security IC Embedded Software and the Secure Flash Loader is not available.

OT.SCD_Secrecy and OT.SCD_Unique require sufficient quality of random numbers for the generation of SCD/SVD, which matches to O.RND.

OT.Tamper_ID, OT.Tamper_Resistance and OT.Prot_Phys-Tamper require detection of and resistance to physical tampering which matches to O.Phys-Probing, O.Phys-Manipulation and O.Malfunction.

The following Platform-objectives are not relevant for or cannot be mapped to the Composite-TOE:

- O.Add-Functions cannot be mapped
- O.MEM_ACCESS is not relevant because the Composite-TOE does not use area based memory access control.

All Security Objectives for the Environment (except for OE.Lim_Block_Loader) (see chapter 4.2, 4.3) are not linked to the platform and are therefore not applicable to this mapping. These objectives are:

- OE.Legislative_Compliance
- OE.Passive_Auth_Sign Authentication of ID_Card by Signature
- OE.Chip_Auth_Key Chip Authentication Key
- OE.Personalisation Personalisation of ID_Card
- OE.Terminal_Authentication Authentication of rightful terminals
- OE.Terminal Terminal operating
- OE.Travel_Document_Holder
- OE.SVD_Auth
- OE.CGA_QCert
- OE.HID_VAD
- OE.DTBS_Intend
- OE.DTBS_Protect
- OE.Code-Confidentiality
- OE.Secure_Environment
- OE.Auth_Key_Travel_Document
- OE.Authoriz_Sens_Data
- OE.Exam_Travel_Document
- OE.Ext_Insp_Systems
- OE.Prot_Logical_Travel_Document
- OE.RestrictedIdentity
- OE.Signatory

- OE.SSCD_Prov_Service
- OE.Eligible_Terminals_Only

There is **no conflict** between **security objectives** of this Composite-ST and the Platform-ST [HWST].

6.4.2.3 Security requirements

6.4.2.3.1 Security Functional Requirements

This Composite-ST has the following platform related SFRs:

- FCS_CKM.1
- FCS_COP.1/PACE_ENC_EAC2PP
- FCS_COP.1/PACE_MAC_EAC2PP
- FCS_COP.1/PACE_MAC_EAC1PP
- FCS_COP.1/PACE_ENC_EAC1PP
- FCS_COP.1/CA_ENC_EAC1PP
- FCS_COP.1/CA_MAC_EAC1PP
- FCS_COP.1/UPD_DEC_MREDONPP
- FCS_COP.1/UPD_ITC_MREDONPP
- FPT_PHP.1/SSCDPP
- FPT_PHP.3/EAC2PP
- FCS_RND.1/EAC2PP
- FPT_EMS.1/EAC2PP
- FPT_EMS.1/SSCDPP
- FPT_EMS.1/UPD_MREDONPP
- FPT_EMS.1/EAC1PP
- FPT_FLS.1/EAC2PP
- FPT_FLS.1/UPD_MREDONPP
- FMT_LIM.1/Loader
- FMT_LIM.2/EAC2PP
- FMT_LIM.2/Loader
- FMT_LIM.1/EAC2PP
- FAU_SAS.1/EAC2PP
- FAU_SAS.1/UPD_MREDONPP
- FDP_SDI.2/Persistent_SSCDPP
- FDP_SDI.2/DTBS_SSCDPP

- FPT_TST.1/EAC2PP
- FPT_TST.1/UPD_MREDONPP
- FCS_CKM.4/EAC2PP

The following Platform-SFRs could be mapped to Composite-SFRs:

- FCS_RNG.1/TRNG
- FRU_FLT.2
- FPT_FLS.1
- FPT_PHP.3
- FCS_COP.1/AES
- FCS_CKM.4/AES
- FDP_SDI.2
- FPT_TST.2
- FMT_LIM.1/2
- FAU_SAS.1
- FCS_CKM.4/TDES (by SCP)
- FCS_COP.1/TDES (by SCP).

They will be mapped as seen in the following table.

PlatformST		FCS_RNG.1/TRNG	FCS_COP.1/AES	FCS_CKM.4/AES	FRU_FLT.2	FPT_FLS.1	FPT_PHP.3	FMT_LIM.1/2	FAU_SAS.1	FDP_SDI.2	FPT_TST.2	FCS_CKM.4/TDES (by SCP)	FCS_COP.1/TDES (by SCP)
Composite-ST	FCS_CKM.1	x											
	FCS_COP.1/PACE_ENC_EAC2PP FCS_COP.1/PACE_MAC_EAC2PP		X										X(only for *)

PlatformST		FCS_RNG.1/TRNG	FCS_COP.1/AES	FCS_CKM.4/AES	FRU_FLT.2	FPT_FLS.1	FPT_PHP.3	FMT_LIM.1/2	FAU_SAS.1	FDP_SDI.2	FPT_TST.2	FCS_CKM.4/TDES (by SCP)	FCS_COP.1/TDES (by SCP)
	FCS_COP.1/PACE_MAC_EAC1PP FCS_COP.1/PACE_ENC_EAC1PP FCS_COP.1/CA_ENC_EAC1PP (*) FCS_COP.1/CA_MAC_EAC1PP (*) FCS_COP.1/UPD_DEC_MREDONPP FCS_COP.1/UPD_ITC_MREDONPP												
	FPT_PHP.1/SSCDPP				X	X	X						
	FPT_PHP.3/EAC2PP				X	X	X						
	FCS_RND.1**/EAC2PP**	X											
	FPT_EMS.1/EAC2PP						X						

PlatformST		FCS_RNG.1/TRNG	FCS_COP.1/AES	FCS_CKM.4/AES	FRU_FLT.2	FPT_FLS.1	FPT_PHP.3	FMT_LIM.1/2	FAU_SAS.1	FDP_SDI.2	FPT_TST.2	FCS_CKM.4/TDES (by SCP)	FCS_COP.1/TDES (by SCP)
	FPT_EMS.1/SSCDPP FPT_EMS.1/UPD_MREDONPP FPT_EMS.1/EAC1PP												
	FPT_FLS.1/EAC2PP FPT_FLS.1/UPD_MREDONPP					X							
	FMT_LIM.1/Loader FMT_LIM.2/EAC2PP FMT_LIM.2/Loader FMT_LIM.1/EAC2PP							X					
	FAU_SAS.1/EAC2PP FAU_SAS.1/UPD_MREDONPP								X				
	FDP_SDI.2/Persistent_SSCDPP									X			
	FDP_SDI.2/DTBS_SSCDPP									X			

PlatformST		FCS_RNG.1/TRNG	FCS_COP.1/AES	FCS_CKM.4/AES	FRU_FLT.2	FPT_FLS.1	FPT_PHP.3	FMT_LIM.1/2	FAU_SAS.1	FDP_SDI.2	FPT_TST.2	FCS_CKM.4/TDES (by SCP)	FCS_COP.1/TDES (by SCP)
	FPT_TST.1/EAC2PP FPT_TST.1/UPD_MREDONPP										X		
	FCS_CKM.4/EAC2PP			X									
	FCS_CKM.4/EAC1_PP			X								X	

Table 11 Mapping of SFRs

FCS_CKM.1 requires sufficient quality of random numbers for the generation of SCD/SVD, which matches to FCS_RNG.1/TRNG.

FCS_COP.1 matches to FCS_COP.1/AES when the AES coprocessor is used by the TOE.

FPT_PHP.1 and FPT_PHP.3 of the composite ST matches the robustness requirements of FRU_FLT.2, FPT_FLS.1 and FPT_PHP.3 of the platform ST.

FCS_CKM.4/TDES (by SCP) and FCS_COP.1/TDES (by SCP) (of the platform match respectively FCS_CKM.4/EAC1PP and (FCS_COP.1/CA_ENC_EAC1PP and FCS_COP.1/CA_MAC_EAC1PP), as the composite uses the 3DES coprocessor.

FMT_LIM.1/2 of the composite TOE matches to the equivalent SFR of the platform TOE.

FAU_SAS.1 of the composite TOE matches its equivalent SFR of the platform.

FDP_SDI.2/Persistent_SSCD and FDP_SDI.2/DTBS_SSCD matches to the equivalent SFR of the platform TOE.

The following Platform-SFRs could not be be mapped to Composite-SFRs:

- FCS_COP.1/RSA because no RSA is used for the composite TOE
- FDP_ACC.1 because the composite TOE is always in system mode and therefore no MMU is necessary and because the composite TOE does not use the platform TOE special function registers.
- FDP_ACF.1 because the composite TOE does not use the platform TOE special function registers and the MMU.
- FMT_MSA.3 because the composite TOE is always in system mode and therefore no MMU is necessary.
- FMT_MSA.1 because the composite TOE is always in system mode and therefore no MMU and special function registers is necessary.
- FMT_SMF.1 because ther TOE does not change the CPU mode.
- FDP_ITT.1 because it deals with the internal data processing policy of the platform TOE that does not by itself impact the composite TOE.
- FPT_ITT.1 because it deals with the basic internal data protection of the platform TOE that does not by itself impact the composite TOE.
- FDP_SDC.1 because it deals with the basic internal data protection of the platform TOE that does not by itself impact the composite TOE.
- FDP_IFC.1 because it deals with the data processing policy of the platform TOE that does not by itself impact the composite TOE.
- FDP_SDI.1 is already covered by FDP_SDI.2.
- FCS_COP.1/ECDH because it does not by itself impact the composite TOE.
- FCS_CKM.1/RSA because it deals with RSA that does not impact the composite TOE.
- FCS_COP.1/ECDSA because the composite TOE does not use the platform TOE cryptographic library.
- FCS_CKM.1/EC because the composite TOE does not use the platform TOE cryptographic library.
- FCS_RNG.1/DRNG because the composite TOE does not use the platform deterministic random number generation
- FCS_RNG.1/KSG because the composite TOE does not use the platform key stream generation.
- FCS_RNG.1/HPRG because the composite TOE does not use the platform hybrid random number generator

- FCS_COP.1/AES-SCL, FCS_CKM.4/AES-SCL, FCS_COP.1/CMAC-SCL-1, FCS_CKM.4/CMAC-SCL-1, FCS_COP.1/TDES-SCL and FCS_CKM.4/TDES-SCL because the composite TOE does not use the platform cryptographic library.
- FDP_UCT.1, FDP_UIT.1, FIA_API.1, FTP_ITC.1, FDP_ACC.1 and FDP_ACF.1 because the ST Flash Loader is used to load the encrypted initialization image into the flash memory of the chips during Initialization (after Phase 4) and Composite Product Integration (in Phase 5). The usage of the Loader is addressed in [AGD_PRE]. In User configuration (Phases 5-6), the Loader capability is not accessible by the Security IC Embedded Software and the Secure Flash Loader is not available.
- FMT_LIM.1 because it is an internal test feature of the IFX platform that is not accessible by the Composite TOE
- FMT_LIM.2 because it is an internal test feature of the IFX platform that is not accessible by the Composite TOE.

6.4.2.3.2 Assurance requirements

The Composite-ST requires EAL 4 according to Common Criteria V3.1R5 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

The Platform-ST has been certified to EAL 6 according to Common Criteria V3.1 R5 augmented by: ALC_FLR.1.

As EAL 6 covers all assurance requirements of EAL 4 all non augmented parts of the Composite-ST will match to the Platform-ST assurance requirements. But also the augmented parts of the Composite-ST match to the Platform-ST.

6.4.3 Overall no contradictions found

Overall there is **no conflict** between **security requirements** of this Composite-ST and the Platform-ST.

7 TOE summary specification

This chapter gives the overview description of the different TOE Security Functions composing the TSF.

7.1 TOE Security Functions

7.1.1 SF_AccessControl

The TOE provides access control mechanisms that allow among others the maintenance of different users (Manufacturer, Personalisation Agent, Country Verifying Certification Authority (CVCA), Document Verifier (DV), domestic Extended Inspection System, foreign Extended Inspection System, Administrator, Signatory). After activation or reset no user is authenticated. The Signatory can authenticate himself using the signature PIN. After 10 unsuccessful consecutive authentication attempts the signature PIN is permanently blocked.

The reuse of authentication data related to PACE Protocol according to [TR03110-2-v2.20], sec. 4.2 and Terminal Authentication Protocol according to [TR03110-2-v2.20], sec. 4.4, Version 2 is prevented.

To support user authentication General Authentication Procedure as the sequence

- PACE Protocol according to [TR03110-2-v2.20], sec. 3.2,
- Terminal Authentication Protocol according to [TR03110-2-v2.20], sec. 3.3, Version 2,
- Chip Authentication Protocol according to [TR03110-2-v2.20], sec. 3.4, Version 2[434], or sec. 3.5, Version3 and
- Secure messaging in encrypt-then-authenticate mode according to [TR03110-3].

Personalization Agent is the only role with the ability if the ePass application is installed:

- to disable read access for users to the Initialization Data.
- to write the initial CVCA Public Key, the initial CVCA Certificate, and the initial Current Date.
- to write the Document Basic Access Keys.
- to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the ePass application after successful authentication.

[434] the Passive Authentication is considered to be part of the Chip Authentication (CA) Protocol within this PP.

The access control mechanisms ensure that only the Country Verifying Certification Authority has the ability to update the CVCA Public Key and the CVCA Certificate.

The access control mechanisms ensure that only authenticated Extended Inspection System with the Read access to

- DG 3 (Fingerprint) is allowed to read the data in EF.DG3 of the ePass application.
- DG 4 (Iris) is allowed to read the data in EF.DG4 of the ePass application.

In all other cases, reading any of the EF.DG3 to EF.DG4 of the ICAO-compliant ePass is explicitly denied.

The access control mechanisms ensure that only the Administrator can generate the signature key pair or export the public signature key in an authentic way for certification. In addition, only the Administrator can store the certificate or certificate information for the public signature key on the TOE. The access control mechanisms also ensure that only the Signatory can set and change the signature PIN or generate electronic signatures using the private signature key.

The access control mechanisms allow the execution of certain security relevant actions (e.g. self-tests) without successful user authentication.

The access control mechanisms allow the storage of Initialisation and Pre-Personalisation Data in audit records through the Manufacturer.

Test Features of the TOE are not available for the user in Phase 4. If Test Features are performed by the TOE then no User Data can be disclosed or manipulated, no TSF data can be disclosed or manipulated, no software can be reconstructed and no substantial information about construction of TSF can be gathered which may enable other attacks.

Only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol and the Access Control.

All security attributes under access control are modified in a secure way so that no unauthorised modifications are possible.

7.1.2 SF_AssetProtection

When the private signature key or the signature PIN are no longer needed in the internal memory of the TOE for calculations these parts of the memory are overwritten.

The TOE supports the calculation of block check values for data integrity checking. These block check values are stored with persistently stored assets residing on the TOE as well as temporarily stored hash values for data that is intended to be signed.

The TOE hides information about IC power consumptions and command execution time, to ensure that no confidential information can be derived from this data.

7.1.3 SF_TSFProtection

The TOE detects physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation. The TOE is resistant to physical tampering of the TSF. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analysing and physical tampering.

The TOE demonstrates the correct operation of the TSF by among others verifying the integrity of the TSF and TSF data and verifying the absence of fault injections. In the case of inconsistencies in the calculation of the signature and fault injections during the operation of the TSF the TOE preserves a secure state.

7.1.4 SF_KeyManagement

The TOE supports onboard generation of corresponding EC-DSA keypairs with key length of 256, 320, 384 and 512 bit. For this the TOE uses random numbers generated by its DRG.4 deterministic random number generator. The TOE also supports onboard generation of cryptographic keys based on the ECDH compliant [TR03111] as well as generation of ECC key pairs.

The TOE supports overwriting the cryptographic keys stored in the flash memory with zero values prior to conclusion of the Personalisation Phase.

The TOE supports the distribution of cryptographic keys in accordance with PACE: as specified in [TR03110-2-v2.20] and CA: as specified in [TR03110-2-v2.20].

7.1.5 SF_SignatureGeneration

The TOE performs ECDSA digital signature verification with SHA-256, SHA-384 and SHA-512 and cryptographic key sizes 256, 384 and 512 bit according to [TR03111] and [FIPS180-4].

The TOE performs digital ECDSA signature generation with SHA-256, SHA-384 and SHA-512 and cryptographic key sizes 256, 320, 384 and 512 bit according to [TR03111] and [FIPS180-4].

7.1.6 SF_TrustedCommunication

The TOE supports the establishment of a trusted channel/path based on mutual authentication with negotiation of symmetric cryptographic keys used for the protection of the communication data with respect to confidentiality and integrity. AES and CMAC, and 3DES and Retail-MAC

are used for encryption and integrity protection of the communication data.

7.2 Assurance Measures

This chapter describes the Assurance Measures fulfilling the requirements listed in chapter 6.3.

The following table lists the Assurance measures and references the corresponding documents describing the measures.

Assurance Measures	Description
AM_ADV	The representing of the TSF is described in the documentation fo functional specification, in the documentation for TOE design, in th security architecture description and in the documentation for implementation representation.
AM_AGD	The guidance documentation is described in the operational user guidance documentation and in the documentation for preparative procedures.
AM_ALC	The life cycle support of the TOE during its development and maintenance is described in the life cycle documentation including configuration management, delivery procedures, development security as well as development tools.
AM_ATE	The testing of the TOE is described in the test documentation..
AM_AVA	The vulnerability assessment for the TOE is described in the vulnerability analysis documentation.

Table 12 References of Assurance measures

7.3 Fulfilment of the SFRs

The following table shows the mapping of the SFRs to security functions of the TOE.

	SF_AccessControl	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement	SF_SignatureGeneration	SF_TrustedCommunication
FCS						
FCS_CKM.1/DH_PACE_EAC2PP				X		
FCS_COP.1/SHA_EAC2PP					X	
FCS_COP.1/SIG_VER_EAC2PP					X	
FCS_COP.1/PACE_ENC_EAC2PP		X				
FCS_COP.1/PACE_MAC_EAC2PP			X			
FCS_CKM.4/EAC2PP				X		
FCS_RND.1/EAC2PP					X	
FCS_CKM.1/CA3				X		
FCS_COP.1/CA3			X			
FCS_CKM.1/DH_PACE_EAC1PP				X		
FCS_CKM.4/EAC1_PP				X		
FCS_COP.1/PACE_ENC_EAC1PP			X			X
FCS_COP.1/PACE_MAC_EAC1PP			X			X
FCS_RND.1/EAC1PP			X			X
FCS_CKM.1/CA_EAC1PP				X		
FCS_COP.1/CA_ENC_EAC1PP			X			X
FCS_COP.1/SIG_VER_EAC1PP			X			X
FCS_COP.1/CA_MAC_EAC1PP			X			X

FCS_CKM.1/CAM				X		
FCS_COP.1/CAM			X			X
FCS_CKM.1/SSCDPP				X		
FCS_CKM.4/SSCDPP				X		
FCS_COP.1/SSCDPP					X	
FCS_COP.1/UPD_ITC_MREDONPP			X			X
FCS_CKM.1/UPD_ITC_MREDONPP				X		
FCS_COP.1/UPD_DEC_MREDONPP			X			X
FCS_CKM.1/UPD_DEC_MREDONPP				X		
FCS_COP.1/UPD_SIG_MREDONPP			X			
FCS_COP.1/UPD_INT_MREDONPP			X			X
FCS_CKM.1/UPD_INT_MREDONPP				X		
FCS_CKM.4/UPD_MREDONPP				X		

Table 13 Mapping of FCS SFRs to mechanisms of TOE

	SF_AccessControl	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement	SF_SignatureGeneration	SF_TtrustedCommunication
Class FIA						
FIA_AFL.1/Suspend_PIN_EAC2PP	X					
FIA_AFL.1/Block_PIN_EAC2PP	X					
FIA_API.1/CA_EAC2PP						X
FIA_API.1/RI_EAC2PP						X
FIA_UID.1/PACE_EAC2PP	X					
FIA_UID.1/EAC2_Terminal_EAC2PP	X					
FIA_UAU.1/PACE_EAC2PP	X					
FIA_UAU.1/EAC2_Terminal_EAC2PP	X					
FIA_UAU.4/PACE_EAC2PP	X					
FIA_UAU.6/CA_EAC2PP	X					
FIA_AFL.1/PACE_EAC2PP	X					
FIA_UAU.6/PACE_EAC2PP	X					
FIA_API.1/CA3						X
FIA_UAU.5/PACE_EAC2PP	X					
FIA_UAU.6/CA3	X					
FIA_UAU.1/PACE_EAC1PP	X					
FIA_UAU.4/PACE_EAC1PP	X					

FIA_UAU.5/PACE_EAC1PP	X					
FIA_UAU.6/PACE_EAC1PP	X					
FIA_UAU.6/EAC_EAC1PP	X					
FIA_API.1/EAC1PP						X
FIA_AFL.1/PACE_EAC1PP	X					
FIA_UID.1/PACE_EAC1PP	X					
FIA_UAU.5/PACE_EAC1PP	X					
FIA_API.1/PACE_CAM						X
FIA_UID.1/SSCDPP	X					
FIA_AFL.1/SSCDPP	X					
FIA_UAU.1/SSCDPP	X					
FIA_AFL.1/UPD_MREDONPP	X					
FIA_UID.1/UPD_MREDONPP	X					
FIA_UAU.1/UPD_MREDONPP	X					

Table 14 Mapping of FIA SFRs to mechanisms of TOE

	SF_AccessControl	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement	SF_SignatureGeneration	SF_TtrustedCommunication
Class FDP						
FDP_ACF.1/TRM	X					
FDP_ACC.1/TRM_EAC2PP	X					
FDP_ACF.1/TRM_EAC2PP	X					
FDP_RIP.1/EAC2PP		X				
FDP_UCT.1/TRM_EAC2PP	X					X
FDP_UIT.1/TRM_EAC2PP	X					
FDP_ACC.1/TRM_EAC1PP	X					
FDP_ACF.1/TRM_EAC1PP	X					
FDP_RIP.1/EAC1PP				X		
FDP_UCT.1/TRM_EAC1PP	X					X
FDP_UIT.1/TRM_EAC1PP	X					
FDP_ACC.1/SCD/SVD_Generation_SSCDPP	X					
FDP_ACF.1/SCD/SVD_Generation_SSCDPP	X					
FDP_ACC.1/SVD_Transfer_SSCDPP	X					
FDP_ACF.1/SVD_Transfer_SSCDPP	X					
FDP_ACC.1/Signature-creation_SSCDPP	X					

FDP_ACF.1/Signature-creation_SSCDPP	X					
FDP_RIP.1/SSCDPP		X				
FDP_SDI.2/Persistent_SSCDPP		X				
FDP_SDI.2/DTBS_SSCDPP		X				
FDP_ACC.1/UPD_MREDONPP	X					
FDP_ACF.1/UPD_MREDONPP	X					
FDP_IFC.1/UPD_MREDONPP		X				
FDP_IFF.1/UPD_MREDONPP		X				
FDP_RIP.1/UPD_MREDONPP		X				

Table 15 Mapping of FDP SFRs to mechanims of TOE

	SF_AccessControl	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement	SF_SignatureGeneration	SF_TtrustedCommunication
Class FTP						
FTP_ITC.1/PACE_EAC2PP						X
FTP_ITC.1/CA_EAC2PP						X
FTP_ITC.1/CA3						X
FTP_ITC.1/PACE_EAC1PP						X
FTP_ITC.1/UPD_MREDONPP						X

Table 16 Mapping of FTP SFRs to mechanisms of TOE

	SF_AccessControl	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement	SF_SignatureGeneration	SF_TtrustedCommunication
Class FAU						
FAU_SAS.1/EAC2PP	X					
FAU_SAS.1/EAC1PP	X					
FAU_SAS.1/UPD_MREDONPP	X					

Table 17 Mapping of FAU SFRs to mechanisms of TOE

	SF_AccessControl	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement	SF_SignatureGeneration	SF_TtrustedCommunication
Class FMT						
FMT_SMR.1	X					
FMT_MTD.1/CVCA_INI_EAC2PP	X					
FMT_MTD.1/CVCA_UPD_EAC2PP	X					
FMT_SMF.1/EAC2PP	X					
FMT_SMR.1/PACE_EAC2PP	X					
FMT_MTD.1/DATE_EAC2PP	X					
FMT_MTD.1/PA_EAC2PP	X					
FMT_MTD.1/SK_PICC_EAC2PP	X					
FMT_MTD.1/KEY_READ_EAC2PP	X					
FMT_MTD.1/Initialize_PIN_EAC2PP	X					
FMT_MTD.1/Change_PIN_EAC2PP	X					
FMT_MTD.1/Resume_PIN_EAC2PP	X					
FMT_MTD.1/Unblock_PIN_EAC2PP	X					
FMT_MTD.1/Activate_PIN_EAC2PP	X					
FMT_MTD.3/EAC2PP		X				
FMT_LIM.1/EAC2PP		X				
FMT_LIM.2/EAC2PP		X				

FMT_MTD.1/INI_ENA_EAC2PP	X					
FMT_MTD.1/INI_DIS_EAC2PP	X					
FMT_SMF.1/EAC1PP	X					
FMT_SMR.1/PACE_EAC1PP	X					
FMT_LIM.1/EAC1PP		X				
FMT_LIM.2/EAC1PP		X				
FMT_MTD.1/INI_ENA_EAC1PP	X					
FMT_MTD.1/INI_DIS_EAC1PP	X					
FMT_MTD.1/CVCA_INI_EAC1PP	X					
FMT_MTD.1/CVCA_UPD_EAC1PP	X					
FMT_MTD.1/DATE_EAC1PP	X					
FMT_MTD.1/CAPK_EAC1PP	X					
FMT_MTD.1/PA_EAC1PP	X					
FMT_MTD.1/KEY_READ_EAC1PP	X					
FMT_MTD.3/EAC1PP		X				
FMT_SMR.1/SSCDPP	X					
FMT_SMF.1/SSCDPP	X					
FMT_MOF.1/SSCDPP	X					
FMT_MSA.1/Admin_SSCDPP	X					
FMT_MSA.1/Signatory_SSCDPP	X					
FMT_MSA.2/SSCDPP	X					
FMT_MSA.3/SSCDPP	X					
FMT_MSA.4/SSCDPP	X					
FMT_MTD.1/Admin_SSCDPP	X					
FMT_MTD.1/Signatory_SSCDPP	X					

FMT_LIM.1/LoaderLimited Capabilities		X				
FMT_LIM.2/LoaderLimited Availability		X				
FMT_SMF.1/UPD_MREDONPP	X					
FMT_MTD.1/UPD_SK_PICC_MREDONPP	X					
FMT_MTD.1/UPD_KEY_READ_MRENONPP	X					
FMT_SMR.1/UPD_MREDONPP	X					

Table 18 Mapping of FMT SFRs to mechanisms of TOE

	SF_AccessControl	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement	SF_SignatureGeneration	SF_TrustedCommunication
Class FPT						
FPT_EMS.1/EAC2PP		X				
FPT_FLS.1/EAC2PP			X			
FPT_TST.1/EAC2PP			X			
FPT_PHP.3/EAC2PP			X			
FPT_TST.1/EAC1PP			X			
FPT_FLS.1/EAC1PP			X			
FPT_PHP.3/EAC1PP			X			
FPT_EMS.1/EAC1PP		X				
FPT_EMS.1/SSCDPP		X				
FPT_FLS.1/SSCDPP			X			
FPT_PHP.1/SSCDPP			X			
FPT_PHP.3/SSCDPP			X			
FPT_TST.1/SSCDPP			X			
FPT_EMS.1 /UPD_MREDONPP		X				
FPT_FLS.1/UPD_MREDONPP			X			
FPT_TST.1/UPD_MREDONPP			X			

Table 19 Mapping of FPT SFRs to mechanisms of TOE

7.3.1 Justifications for the correspondence between functional requirements and TOE mechanisms

Each TOE security functional requirement is implemented by at least one TOE mechanism. In section 7.1 the implementing of the TOE security functional requirement is described in form of the TOE mechanism.

8 Glossary and Abbreviations

8.1 Glossary

Accurate Terminal Certificate
: A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the electronic document's chip to produce terminal certificates with the correct certificate effective date, see [TR03110-3].

Card Access Number (CAN)
: A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the electronic document), semi-static (e.g. printed on a label on the electronic document) or dynamic (randomly chosen by the electronic electronic document and displayed by it using e.g. ePaper, an OLED or similar technologies), cf. [TR03110-2].

Card Security Object (SO_C)
: An RFC3369 CMS signed data structure signed by the Document Signer. It is stored in the electronic document (EF.CardSecurity, see [TR03110-3]) and carries the hash values of different data groups as defined. It also carries the Document Signer Certificate [TR03110-3].

Certificate Chain
: Hierarchical sequence of Terminal Certificate (lowest level), DV Certificate and CVCA Certificates (highest level), where the certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level. The CVCA Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).

Country Verifying Certification Authority (CVCA)
: An organization enforcing the privacy policy of the electronic document issuer with respect to protection of sensitive user data that are stored in the electronic document. Practically, this policy is enforced when a terminal tries to get access to these sensitive user data. The CVCA represents the country specific root of the PKI for EAC1 terminals, EAC2 terminals resp. and creates DV certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA link-certificates, see [TR03110-3].

Current Date
: The most recent certificate effective date contained in a valid CVCA link certificate, a DV certificate or an accurate terminal certificate known to the TOE, see [TR03110-3].

CV Certificate
: Card verifiable certificate according to [TR03110-3].

CVCA Link Certificate
: Certificate of the new public key of the CVCA signed with the old public key of the CVCA where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.

Document Security Object (SO_D)
: A RFC3369 CMS signed data structure, signed by the Document Signer. Carries the hash values of the data groups. It is usually stored in an ICAO-conformant ePass application of an electronic document. It may carry the document signer certificate; see [TR03110-3] and [ICAO9303].

Document Signer
An organization enforcing the policy of the CSCA and signing the electronic document security object stored on the electronic document for passive authentication.A document signer is authorized by the national CSCA to issue document signer certificate, cf. [TR03110-3] and [ICAO9303]. This role is usually delegated to the personalization agent.

Document Verifier (DV)
An organization issuing terminal certificates as a Certificate Authority, authorized by the corresponding CVCA to issue certificates for EAC1 terminals, EAC2 terminals resp., see [TR03110-3].

Extended Access Control 1
A set of security protocols and mechanisms to ensure genuineness of the electronic document and to allow a fine-grained access control to sensitive user data stored on an electronic document [TR03110-1].

Extended Access Control 2
A set of security protocols and mechanisms to ensure genuineness of the electronic document and to allow a fine-grained access control to sensitive user data stored on an electronic document [TR03110-2].

IC Dedicated Software
Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different entities. The usage of parts of the IC dedicated software might be restricted to certain life phases.

IC Embedded Software
Software embedded in an IC and not being designed by the IC developer. The IC embedded software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.

Electronic Document (electronic part only)
A smart card integrated into a plastic, optical readable cover. An electronic electronic document provides one or several application(s), such as an eID application, or an ePass application.

Initialization Data
Any data defined by the electronic document manufacturer and injected into the non-volatile memory by the integrated circuit manufacturer. These data are, for instance, used for traceability and for IC identification as IC_Card material (IC identification data).

Issuing State
The country issuing the electronic document; see [ICAO9303].

Machine Readable Zone (MRZ)
Fixed dimensional area located on the front of an ICAO-conformant electronic document. The MRZ contains mandatory and optional data for machine reading using optical character recognition; see [ICAO9303].The MRZ-Password is a secret key that is derived from the machine readable zone and may be used for PACE.

Meta-Data of a CV Certificate
Data within the certificate body as described in [TR03110-3]. The meta-data of a CV certificate comprise the following elements:
•Certificate Profile Identifier,
•Certificate Authority Reference,
•Certificate Holder Reference,
•Certificate Holder Authorization Template (CHAT),

- Certificate Effective Date,
- Certificate Expiration Date,
- Certificate Extensions (optional).

Passive Authentication
Security mechanism implementing (i) verification of the digital signature of the card (document) security object and (ii) comparing the hash values of the read data fields with the hash values contained in the card (document) security object. See [TR03110-3].

Password Authenticated Connection Establishment (PACE)
A communication establishment protocol defined in [TR03110-2] / [ICAO9303] resp.

PACE Password
A password needed for PACE authentication, e. g. CAN, MRZ, or a PIN.

Personal Identification Number (PIN)
A short secret password being only known to the electronic document holder. The PIN is a blocking password, see [TR03110-2].

Personalization
The process by which data related to the electronic document holder (biographic and biometric data, or key pair(s) for a potential signature application) are stored in and unambiguously, inseparably associated with the electronic document.

PIN Unblock Key (PUK)
A long secret password being only known to the electronic document holder. The PUK is a non-blocking password, see [TR03110-2].

Pre-personalization Data
Any data that is injected into the non-volatile memory of the TOE by the manufacturer for traceability of the non-personalized electronic document and/or to secure shipment within or between the life cycle phases manufacturing and card issuing.

Restricted Identification
Restricted Identification is a mechanism consisting of a security protocol for pseudo anonymization. This is achieved by providing a temporary electronic document identifier specific for a terminal sector and supporting related revocation features (see [TR03110-2]).

Secure Messaging
Secure messaging using encryption and message authentication code according to [ISO7816-4].

8.2 Abbreviations

ATT	Authentication Terminal as defined in [TR03110-2], sec. 2.1
BAC	Basic Access Control
BIS	Basic Inspection System
CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
CGA	Certificate generation application, please refer to [SSCDPP]. In the current context, it is represented by ATT for the eSign application.
CHAT	Certificate Holder Authorization Template
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority

DS	Document Signer
DTBS	Data to be signed, please refer to [SSCDPP]
DTBS/R	Data to be signed or its unique representation, please refer to [SSCDPP]
DV	Document Verifier
EAC	Extended Access Control
EF	Elementary file
HID	Human Interface Device, please refer to [SSCDPP]. It is equivalent to SGT in the current context.
MF	Master File
MRTD	Machine Readable Travel Document
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organizational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PIN	Personal Identification Number
PP	Protection Profile
PUK	PIN Unblock Key
RAD	Reference Authentication Data, please refer to [SSCDPP]
RF	Radio Frequency
SAC	Supplemental Access Control
SAR	Security assurance requirements
SCA	Signature creation application, please refer to [SSCDPP]. It is equivalent to SGT in the current context.
SCD	Signature Creation Data, please refer to [SSCDPP]; the term ‘private signature key within the eSign application’ is synonym within the current ST.
SFR	Security functional requirement
SGT	Signature Terminal
SPD	Security Problem Definition
SVD	Signature Verification Data, cf. [SSCDPP]. The public key to verify a signature.
TA	Terminal Authentication
TOE	Target of Evaluation
TSF	TOE security functionality
TSP	TOE Security Policy (defined by the current document)
VAD	Verification Authentication Data, cf. [SSCDPP]

9 Reference Documentation

AGD_PRE	Guidance Documentation for the Personalisation Phase STARCOS 3.7 ID C1, Version 1.6 / Status 06.07.2020, Giesecke+Devrient Mobile Security GmbH
AIS20	Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20, „Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren“, Version 3 vom 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik (BSI)
AIS31	Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, „Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren“, Version 3 vom 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik (BSI)
CC1	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, 3.1, Revision 5
CC2	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, 3.1, Revision 5
CC3	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, 3.1, Revision 5
CC4	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004 , 3.1, Revision 5
COMPEVAL	Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, December 2015, Version 1.4, CCDB-2015-12-001.
EAC1PP	BSI: Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012 v1.3.2 (5. December 2012)
EAC2PP	BSI: Common Criteria Protection Profile - ID-Card implementing Extended Access Control 2 as defined in BSI TR-03110, BSI-CC-PP-0086-2015 v1.01 (May 20th, 2015)
FIPS180-4	National Institute of Standards and Technology: FIPS PUB

	180-4: Secure hash standard, August 2015.
FIPS 197	National Institute of Standards and Technology: FIPS PUB 197: Avanced Encryption Standard (AES), November 2001.
HUiF	Update im Feld-Harmonisierung,T-Systems International, Version 0.4, 09.04.2018
HWST	Public Security Target BSI-DSZ-CC-1110-V3-2020, “Public Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h design step H13”(sanitised public document), Infineon Technologies AG, Version 1.8, 22-04-2020.
ICAO9303	ICAO: ICAO Doc 9303 - Machine Readable Travel Documents, 7th edition, 2015
ICAOMRTDTR	International Civil Aviation Organization, ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, November 2010
ICPP	Inside Secure, Infineon Technologies AG, NXP Semiconductors Germany GmbH, STMicroelectronics: Common Criteria Protection Profile - Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, v1.0 (13.01.2014)
ISO14443	ISO/IEC 14443 Identification cards — Contactless integrated circuit cards,
ISO7816-4	ISO/IEC 7816-4:2013 Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange,
MR.ED2.0	BSI: Common Criteria Protection Profile - Machine Readable Electronic Documents based on BSI TR03110, BSI-CC-PP-0087-V2-2016-MA-01
MR.ED-ON-PP	BSI: Common Criteria Protection Profile - Machine Readable Electronic Documents - Optionales Nachladen (Optional Post-Emission Updates), BSI-CC-PP-0090-2016 v0.9.2 (August 18th, 2016)
PACEPP	BSI: Common Criteria Protection Profile - Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011
PKCS#3	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, November 1, 1993

SSCDPP	CEN: Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation, EN 419211-2:2013, BSI-CC-PP-0059-2009-MA-02, July 2013
TR03110-1	BSI: TR-03110-1 - Advanced Security Mechanisms for Machine Readable Travel Documents. Part 1 - eMRTDs with BAC/PACEv2 and EACv1, v2.10 (20. March 2012)
TR03110-2	BSI: TR-03110-2 - Advanced Security Mechanisms for Machine Readable Travel Documents. Part 2 - Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI) v2.10 (20. March 2012)
TR03110-2-v2.20	BSI: 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), v2.20 (3. February 2015)
TR03110-3	BSI: TR-03110-3 - Advanced Security Mechanisms for Machine Readable Travel Documents. Part 3 - Common Specifications v2.10 (20. March 2012)
TR03111	Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, version 2.10, 01.06.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)
TR3116-2	Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 2: eID-Karten und hoheitliche Dokumente Stand 2020 Datum: 27. Januar 2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)