ID&TRUST

IDENTITY APPLET V3.4-P2/EIDAS

ELECTRONIC IDENTITY CARD WITH PACE-GM, PACE-CAM, EXTENDED ACCESS CONTROL V1 AND V2, RESTRICTED IDENTIFICATION AND ACTIVE AUTHENTICATION

SECURITY TARGET

COMMON CRITERIA / ISO 15408

EAL4+

2022

Classification: Public

Revision history

Version	Date	Information
V1.00	18.08.2020	Final version
V1.01	16.09.2020	Minor modification
V1.02	13.10.2020	Update references
V1.03	13.05.2022	Updated TOE identification data, TOE name, ST Title, TOE Description and Bibliography.
V1.04	19.07.2022	Update Bibliography and Platform’s Certification IDs.
v1.05	19.09.2022	Update Bibliography and Platform’s Certification IDs.
v1.06	01.02.2023	Update Bibliography and TOE Reference

Table of Contents

List of Tables

1. ST Introduction

This section provides document management and overview information required to register the Security Target (ST) and to enable a potential user of the ST to determine, whether the ST is of interest.

1.1. ST Reference

Title:	Security Target ID&Trust IDentity Applet v3.4-p2/eIDAS - Electronic Identity Card with PACE-GM, PACE-CAM, Extended Access Control v1 and v2, Restricted Identification and Active Authentication
Author:	ID&Trust Ltd.
Version Number:	v1.06
Date:	01.02.2023

1.2. TOE Reference

The Security Target refers to the product "ID&Trust IDentity Applet Suite v3.4" for CC evaluation.

TOE Name:	IDentity Applet v3.4-p2/eIDAS on NXP JCOP 4 P71
TOE short name:	IDentity Applet v3.4/eIDAS
TOE Identification Data:	
Applet version number	IDentity Applet V3.4/eIDAS v3.4.7470
Patch version number:	024A
Evaluation Criteria:	[4]
Evaluation Assurance Level:	EAL EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 as defined in [3].

Developer: ID&Trust Ltd.

Evaluation Sponsor: NXP Semiconductors Germany GmBH, Troplowitzstraße 20, 22529 Hamburg, Germany

1.3.TOE Overview

This ST claims strict conformance to [5], [6], [13] and [20]. There, slightly different terminology is used. For the ease of understanding, Table 1 gives a brief translation for the used terminology. Compound words that contain terminology of the table should be replaced accordingly.

This ST	PACE PP [13]	EAC1PP [5]	EAC2PP [6]
electronic document	travel document	travel document	electronic document
electronic document presenter	traveler	traveler	electronic document presenter
EAC1 protected data	-	sensitive (user) data	-
EAC2 protected data	-	-	Sensitive User Data
common user data	user data	user data	common user data
PACE terminal	BIS-PACE	BIS-PACE	PACE terminal
EAC1 terminal	-	Extended Inspection System	-
EAC2 terminal	-	-	EAC2 terminal

Table 1 Overview of identifiers of current ST and PPs

1.3.1. TOE Type

IDentity Applet Suite v3.4 is a highly configurable eID solution. It is able to satisfy multiple different application requirements even within a single applet instance. The Application part of the TOE, the applet functionalities are distributed according to the following table:

Application	Function	Standard	Protection Profile (certified or in progress)
IDentity/PKI	Flexible PKI token	CEN TS 14890-1/2 IAS-ECC 1.0.1 [30]	-
IDentity/IAS	European card for e-Services and National e-ID applications	CEN/TS 15480- IAS-ECC 1.0.1 [30]	-
IDentity/QSCD	Qualified Signature Creation Device	CEN/TS 15480-2 IAS-ECC 1.0.1 [30] REGULATION (EU) No 910/2014	[14] [15]

		BSI TR-03117	
IDentity/IDL	International Driving License	ISO/IEC 18013	-
IDentity/EDL	European Driving License	2012/383/EC	-
IDentity/eVR	Electronic Vehicle Registration	1999/37/EC	-
IDentity/eHC	Electronic Health Insurance	CEN/CWA 15794	-
IDentity/BAC	Basic Access Control (BAC)	ICAO Doc 9303 [8]	BSI-CC-PP-0055
IDentity-J	Basic Access Control (BAC) Password Authenticated Connection Establishment (PACE)	ICAO Doc 9303 [8]	JISEC500 [32] JISEC499 [33]
IDentity/PACE-EAC1	Password Authenticated Connection Establishment (PACE) Extended Access Control v1 (EAC1)	ICAO Doc 9303 [8] ICAO TR-SAC [7] BSI TR-03110 v2.21 [16][17][18][19]	BSI-CC-PP-0068-V2-2011 [13] BSI-CC-PP-0056-V2-2012 [5]
IDentity/eIDAS	Password Authenticated Connection Establishment (PACE) Extended Access Control v2 (EAC2)	ICAO TR-SAC [7] BSI TR-03110 v2.21 [16][17][18][19]	BSI-CC-PP-0087 [20]

Table 2 IDentity Applet Suite v3.4 functionalities

All the functions are supplied by the applet “IDentity Applet Suite v3.4”, the behaviour of the applet changes according to the configuration applied during the personalization phase of IDentity Applet life cycle and the environmental behaviour of the usage phase.

The scope of the current ST is only concerned with applet behaviour of configuration IDentity Applet v3.4/eIDAS.

The Target of Evaluation (TOE) is contactless smart card with the IDentity Applet Suite v3.4 configured as IDentity Applet v3.4/eIDAS. The TOE is applicable as an electronic document (with three applications: ePassport, eID and eSign), which compliance to relevant eIDAS standards [16], [17], [18] and provide all necessary security protocols (such as PACE, EAC1, EAC2, etc).

1.3.2. TOE Definition and Operational Usage

The Target of Evaluation (TOE) is a smartcard programmed according to [16] [17]. The smartcard contains multiple applications (at least one). 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:

- *EAC1-protected data*: Sensitive User Data protected by EAC1 (cf. [16]),
- *EAC2-protected data*: Sensitive User Data protected by EAC2 (cf. [17]), and
- *all other (common) user data:* Other user data are protected by Password Authenticated Connection Establishment (PACE, cf. also [17]). Note that EAC1 recommends, and EAC2 requires prior execution of PACE.

1. Application note (taken from [20], application note 1.)

Due to migration periods, some developers have to implement products that function-ally support both PACE and Basic Access Control (BAC), i.e. Supplemental Access Control (SAC) [8].However, any product using BAC is not conformant to the current ST; i.e. the TOE may functionally support BAC, but, while performing BAC, it is acting outside of the security policy defined by the current ST.

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.

Application considered in [16] and [17] are

1. an electronic passport (ePass) application
2. an electronic identity (eID) application, and
3. a signature (eSign) application.

The TOE shall comprise at least:

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, and
5. the associated guidance documentation.

2. Application note (taken from [20], 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 might be considered as a part of the TOE. The decision upon this is up to the certification body in charge that defines the evaluation methodology for the assessment of the contactless interface.

1.3.3. 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, if the TOE contains an eSign application.
- Optionally support the Active Authetnication and Chip Authentication mapping.

1.3.4. 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 [12] and [11]; the latter only if the card has a contactless interface. Akin to [16] and [17] the TOE shall be able to recognize the following terminal types:

PACE terminal

A PACE terminal is a basic inspection system according to [16], [17] resp. It performs the standard inspection procedure, i.e. PACE followed by Passive Authentication, cf. [16]. Afterwards user data are read by the terminal. A PACE terminal is allowed to read only common user data.

For more information see: PACE Terminal

EAC1 terminal

An EAC1 terminal is an extended inspection system according to [16]. It performs the advanced inspection procedure ([16]) 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.

For more information see: EAC1 Terminal / EAC2 Terminal

EAC2 terminal

An EAC2 terminal is an extended inspection system performing the general authentication procedure according to [17] 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.

For more information see: EAC1 Terminal / EAC2 Terminal

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 [18]. 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 [18].

The term terminal within this ST usually refers to any kind of terminal, if not explicitly mentioned otherwise.

The current TOE knows three different configuration as described in 1.4.5 Features of the IDentity Applet. According to the each configuration the following tables give an overview which of the above terminals are related to what application, and which data group is accessible.

European Passport configuration

Terminal/Application	ePassport	eID	eSign

PACE terminal	Common user data	n.a.	n.a.
EAC1 terminal	Common user data and EAC1 protected data	n.a.	n.a.
EAC2 terminal	none	n.a.	n.a.

Identity Card with Protected MRTD Application configuration

Terminal/Application	ePassport	eID	eSign
PACE terminal	none	none	none
EAC1 terminal	none	none	none
EAC2 terminal	Common user data EAC2 protected data	Common user data EAC2 protected data	EAC2 protected data

Identity Card with EU-compliant MRTD Application configuration

Terminal/Application	ePassport	eID	eSign
PACE terminal	Common user data	None	None
EAC1 terminal	Common user data and EAC1 protected data	None	None
EAC2 terminal	none	common user data EAC2 protected data	EAC2 protected data

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

1.4. TOE Description

1.4.1. Product Type

The TOE type addressed by the current ST is a smartcard programmed according to [16] and [17]. The smartcard contains IDentity Applet v3.4/eIDAS, which may be contain multiple applications (at least one). The smartcard with IDentity Applet v3.4/eIDAS is called an electronic document as a whole.

Justification: TOE type definitions of the claimed PPs ([5], [6], [14]) differ slightly. We argue that these differences do not violate consistency:

The TOE type defined both in [5] and [6] is a smartcard. Whereas [5] references [16] (and also [8] and related ICAO specifications, however [16] 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, [17] is given as a reference in [6]. Reference [16] defines the EAC1 protocol, whereas EAC2 is defined in [17]. 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 [5] is here understood in a more broader sense (cf. also Table 1), since the document can also be used in contexts other than just traveling.

The TOE type definition given in [14] 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 [14].

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 [20]. 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 current ST. Conformance with [20] 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

1.4.2. COMPONENTS OF THE TOE

Micro Controller

The Micro Controller is a secure smart card controller from NXP from the SmartMX3 family. The Micro Controller contains a co-processor for symmetric cipher, supporting DES operations and AES, as well as an accelerator for asymmetric algorithms. The Micro Controller further contains a physical random number generator. The supported memory technologies are volatile (Random Access Memory (RAM)) and non-volatile (Read Only Memory (ROM) and FLASH) memory. Access to all memory types is controlled by a Memory Management Unit (MMU) which allows to separate and restrict access to parts of the memory.

IC dedicated software – Micro Controller Firmware

The Micro Controller Firmware is used for testing of the Micro Controller at production, for booting of the Micro Controller after power-up or after reset, for configuration of communication devices and for writing data to non-volatile memory.

IC dedicated software – Crypto Library

The Crypto Library provides implementations for symmetric and asymmetric cryptographic operations, hashing, the generation of hybrid deterministic and hybrid physical random numbers and further tools like secure copy and compare. The supported asymmetric cryptographic operations are ECC and RSA. These algorithms use the Public Key Crypto Coprocessor (PKCC) of the Micro Controller for the cryptographic operations.

Micro Controller, IC dedicated software (Micro Controller Firmware, Crypto Library) are covered by the following certification: Certification ID: BSI-DSZ-CC-1136-V3-2022

Evaluation level EAL6+ ALC_FLR.1 and ASE_TSS.2 according to Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-00084-2014.

IC Embedded Software

Certification ID: CC-22-180212/2

JCOP4 consists of Java Card Virtual Machine (JCVM), Java Card Runtime Environment (JCRE), Java Card API (JCAPI), Global Platform (GP) framework, Configuration Module, etc.

OS Name: JCOP 4 Operating System

Applied OS configuration: Banking & Secure ID

Product Identification: JCOP 4 v4.7 R1.01.4

Evaluation Level: CC EAL 6+ with ASE_TSS.2, ALC_FLR.1 according to Java Card System – Open Configuration Protection Profile, version 3.0.5, Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI, BSI-CC-PP-0099-2017).

Platform UGD: [24]

ID&Trust IDentity Applet Suite – accomplishing IDentity Applet v3.4/eIDAS

Product name: ID&Trust IDentity Applet Suite

Version: 3.4

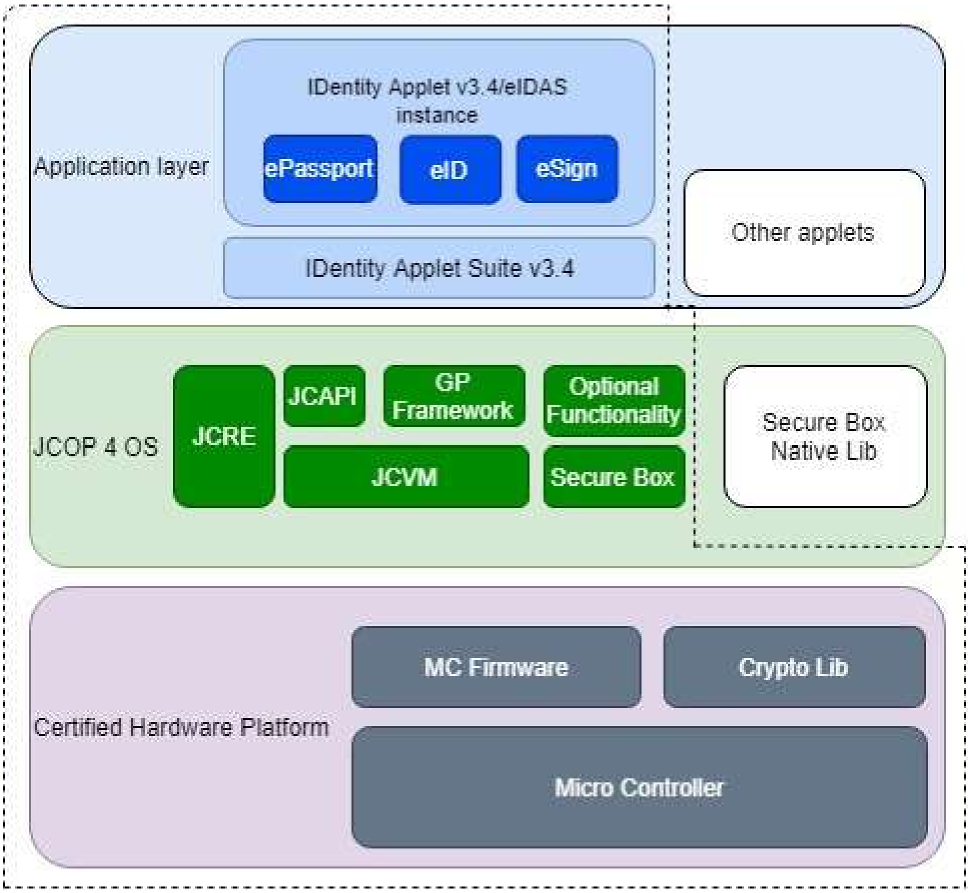
330 Application name[1]: IDentity Applet v3.4/eIDAS

331 TOE Guidance
332 Documentation: [2] IDentity Applet Administrator’s Guide [21]

333 IDentity Applet User’s Guide [22]

334 The composite part always means IDentity Applet v3.4/eIDAS

335 The logical architecture of the TOE:

336 

337 1. Figure TOE Boundaries

338 The TOE is a composite TOE and the dashed line denotes the whole TOE. The underlying certified hardware platform and JCOP 4 OS are marked with purple and green. In this ST the common short name of certified hardware platform and JCOP 4 OS is Platform.

341 The blue box marks the application layer. The ID&Trust IDentity Applet Suite v3.4 could be loaded in the Flash. During the creation phase an instance is created in the Flash and after

[1] The applet is provided in cap file format.
[2] The AGD documents provided in electronic document format.

several configuration steps it will be personalized as IDentity Applet v3.4/eIDAS. For details please see: section 1.4.3 TOE life cycle and [23].

The boxes marked with white are not certified.

1.4.3. TOE Life Cycle

The TOE life cycle is described in terms of the above mentioned four life cycle phases. Akin to [10], the TOE life-cycle is additionally subdivided into seven steps.

Phase 1: Development

Step 1

The TOE is developed in phase 1. NXP 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 operating system is developed by NXP as well. The IDentity Applet v3.4 is developed by ID&Trust Ltd.

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 or in FLASH.

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 [12]. 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.

3. Application note (taken from [20], Application Note 3)

TSF data are data for the operation of the TOE upon which the enforcement of the SFRs relies [1]. 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.

4. Application note (taken from [20], application note 4)

This ST considers at least the first phase and parts of the second phase, i.e. Step 1 up to Step 3, as part of the evaluation. Therefore, the TOE delivery is defined to occur, according to CC, after Step 3. 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.

1.4.4. TOE Security Functions

TSF	Description
TSF.AccessControl	The TOE enforces access control in order to ensure only for authorised users to access User Data and TSF-data and maintains different security roles.

TSF.Authenticate	The TOE supports several authentication mechanisms in order to authenticate the Users, Terminals and to prove the genuineness of the electronic document. The supported mechanism and protocols are based on ICAO and BSI standards [7], [8], [16], [17] and [18].
TSF.SecureManagement	The TOE enforces the secure management of the security attributes, data and functions. Furthermore the TOE restricts the available commands in each TOE life-cycle phase.
TSF.CryptoKey	The TOE uses several cryptographic services such as digital signature creation and verification, asymmetric and symmetric cryptography, random number generation and complete key management.
TSF.AppletParametersSign	The TOE enforces the integrity of itself in each life cycle phases.
TSF.Platform	The TOE relies on the certified functions and services of the Platform. This TSF is collection of those SFRs, which are uses these functions and services.

1.4.5. Features of the IDentity Applet

Taking into consideration the [20] the current ST makes distinct the following configuration:

- European Passport
- Identity Card with Protected MRTD Application
- Identity Card with EU-compliant MRTD Application

1.4.5.1. European Passport

Passwords

- MRZ [16]
- CAN [16]

Authentication Procedure

This configuration requires implementation t the following Authentication Procedure for access to DG3 and DG4 (Sensitive User Data) of the ePassport Application:

- Advanced Inspection procedure [16]

Applications

- ePassport Application

Protocols

- PACE (Generic Mapping, Integrated Mapping and Chip Authentication Mapping) [9], [16]
- Active Authentication [7] (optionally)
- EAC1 [16]

448 ○ Terminal Authentication version 1 [16]

449 ○ Chip Authentication version 1 [16]

450 Data Groups

451 According to [16].

452 Data types in:

453 - Common user data: All DG, which require only BAC/PACE protocol

454 - EAC1 protected data: All DG,which require EAC1 protocol

455 The authorization level of EAC1 terminal is determined by the effective authorization calculated
456 by from the certificate chain.

457 Terminals and access control

Data types	PACE terminal	EAC1 terminal	EAC2 terminal
common user data	X	X	-
EAC1 protected data	-	X	-

458 Table 3 Terminals and access control in European Passport

459 Security Functional Requirements

TOE SFR / Application	ePassport
FCS_CKM.1/DH_PACE_EAC2PP	-
FCS_COP.1/SHA_EAC2PP	-
FCS_COP.1/SIG_VER_EAC2PP	-
FCS_COP.1/PACE_ENC_EAC2PP	-
FCS_COP.1/PACE_MAC_EAC2PP	-
FCS_CKM.4/EAC2PP	-
FCS_RND.1/EAC2PP	-
FCS_CKM.1/DH_PACE_EAC1PP	X
FCS_CKM.4/EAC1PP	X
FCS_COP.1/PACE_ENC_EAC1PP	X
FCS_COP.1/PACE_MAC_EAC1PP	X
FCS_RND.1/EAC1PP	X
FCS_CKM.1/CA_EAC1PP	X
FCS_COP.1/CA_ENC_EAC1PP	X
FCS_COP.1/SIG_VER_EAC1PP	X
FCS_COP.1/CA_MAC_EAC1PP	X
FCS_CKM.1/CA2	-
FCS_CKM.1/RI	-
FCS_CKM.1/AA	X
FCS_COP.1/AA	X
FCS_CKM.1/CAM	X
FCS_COP.1/CAM	X
FCS_CKM.1/SSCDPP	-
FCS_COP.1/SSCDPP	-
FIA_AFL.1/Suspend_PIN_EAC2PP	X

FIA_AFL.1/Block_PIN_EAC2PP	X
FIA_API.1/CA_EAC2PP	-
FIA_API.1/RI_EAC2PP	-
FIA_UID.1/PACE_EAC2PP	-
FIA_UID.1/EAC2_Terminal_EAC2PP	-
FIA_UAU.1/PACE_EAC2PP	-
FIA_UAU.1/EAC2_Terminal_EAC2PP	-
FIA_UAU.4/PACE_EAC2PP	-
FIA_UAU.5/PACE_EAC2PP	-
FIA_UAU.6/CA_EAC2PP	-
FIA_AFL.1/PACE_EAC2PP	-
FIA_UAU.6/PACE_EAC2PP	-
FIA_UID.1/PACE_EAC1PP	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_API.1/PACE_CAM	X
FIA_API.1/AA	X
FIA_AFL.1/PACE_EAC1PP	X
FIA_UID.1/SSCDPP	-
FIA_AFL.1/SSCDPP	-
FIA_UAU.1/SSCDPP	-
FDP_ACC.1/TRM_EAC2PP	-
FDP_ACF.1/TRM	X
FDP_RIP.1/EAC2PP	-
FDP_UCT.1/TRM_EAC2PP	-
FDP_UIT.1/TRM_EAC2PP	-
FDP_ACC.1/TRM_EAC1PP	X
FDP_RIP.1/EAC1PP	X
FDP_UCT.1/TRM_EAC1PP	X
FDP_UIT.1/TRM_EAC1PP	X
FDP_ACC.1/SCD/SVD_Generation_SSCDPP	-
FDP_ACF.1/SCD/SVD_Generation_SSCDPP	-
FDP_ACC.1/SVD_Transfer_SSCDPP	-
FDP_ACF.1/SVD_Transfer_SSCDPP	-
FDP_ACC.1/Signature-creation_SSCDPP	-
FDP_ACF.1/Signature-creation_SSCDPP	-
FDP_RIP.1/SSCDPP	-
FDP_SDI.2/Persistent_SSCDPP	-
FDP_SDI.2/DTBS_SSCDPP	-
FTP_ITC.1/PACE_EAC2PP	-
FTP_ITC.1/CA_EAC2PP	-
FTP_ITC.1/PACE_EAC1PP	X
FAU_SAS.1/EAC2PP	-
FAU_SAS.1/EAC1PP	X
FMT_MTD.1/CVCA_INI_EAC2PP	-
FMT_MTD.1/CVCA_UPD_EAC2PP	-
FMT_SMF.1/EAC2PP	-

FMT_SMR.1	X
FMT_MTD.1/DATE_EAC2PP	-
FMT_MTD.1/PA_EAC2PP	-
FMT_MTD.1/SK_PICC_EAC2PP	-
FMT_MTD.1/KEY_READ_EAC2PP	-
FMT_MTD.1/Initialize_PIN_EAC2PP	-
FMT_MTD.1/Change_PIN_EAC2PP	-
FMT_MTD.1/Resume_PIN_EAC2PP	-
FMT_MTD.1/Unblock_PIN_EAC2PP	-
FMT_MTD.1/Activate_PIN_EAC2PP	-
FMT_MTD.3/EAC2PP	-
FMT_SMR.1/SSCDPP	-
FMT_SMF.1/SSCDPP	-
FMT_MOF.1/SSCDPP	-
FMT_MSA.1/Admin_SSCDPP	-
FMT_MSA.1/SignatorySSCDPP	-
FMT_MSA.2/SSCDPP	-
FMT_MSA.3/SSCDPP	-
FMT_MSA.4/SSCDPP	-
FMT_MTD.1/Admin_SSCDPP	-
FMT_MTD.1/Signatory_SSCDPP	-
FMT_LIM.1/EAC2PP	-
FMT_LIM.2/EAC2PP	-
FMT_MTD.1/INI_ENA_EAC2PP	-
FMT_MTD.1/INI_DIS_EAC2PP	-
FMT_SMF.1/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_LIM.1/Loader	X
FMT_LIM.2/Loader	X
FMT_MTD.1/AA_Private_Key	X
FPT_EMS.1/EAC2PP	-
FPT_FLS.1/EAC2PP	-
FPT_TST.1/EAC2PP	-
FPT_PHP.3/EAC2PP	-
FPT_TST.1/EAC1PP	X
FPT_FLS.1/EAC1PP	X
FPT_PHP.3/EAC1PP	X
FPT_EMS.1/EAC1PP	X
FPT_EMS.1/SSCDPP	-
FPT_FLS.1/SSCDPP	-
FPT_PHP.1/SSCDPP	-
FPT_PHP.3/SSCDPP	-
FPT_TST.1/SSCDPP	-

1.4.5.2. *Identity Card with Protected MRTD Application*

Passwords

- MRZ [16]
- CAN [16]
- PIN [17]
- PUK [17]

While it is technically possible to grant access to the electronic signature functionality by inputting only CAN, this technical option is not allowed in this ST. This is due to the fact that solely the signatory – which is here the Electronic Document Holder – shall be able to generate an electronic signature on his own behalf.

Authentication Procedure

This configuration requires implementation at the following Authentication Procedure for access any User Data stored on the TOE:

- General Authentication Procedure [17]

Applications

- ePassport Application
- eID Application
- eSign Application

Protocols

- PACE (Generic Mapping, Integrated Mapping) [17]
- EAC2 [17]
  - Terminal Authentication version 2 [17]
  - Chip Authentication version 2 [17]
- Restricted Identification [17]

Data Groups

According to [17].

According to [9] and [16].

Data type in:

- EAC2 protected data: All DG in ePassport, eID and eSign application.

489 The authorization level of EAC2 terminal is determined by the effective authorization calculated
490 by from the certificate chain.

491 Terminals and access control

Data type	PACE terminal	EAC1 terminal	EAC2 terminal
Common user data	-	-	X
EAC2 protected data	-	-	X

492 Table 4 Terminals and access control in Identity Card with Protected MRTD Application

TOE SFR / Application	ePassport	eID	eSign
FCS_CKM.1/DH_PACE_EAC2PP	X	X	X
FCS_COP.1/SHA_EAC2PP	X	X	X
FCS_COP.1/SIG_VER_EAC2PP	X	X	X
FCS_COP.1/PACE_ENC_EAC2PP	X	X	X
FCS_COP.1/PACE_MAC_EAC2PP	X	X	X
FCS_CKM.4/EAC2PP	X	X	X
FCS_RND.1/EAC2PP	X	X	X
FCS_CKM.1/DH_PACE_EAC1PP	-	-	-
FCS_CKM.4/EAC1PP	-	-	-
FCS_COP.1/PACE_ENC_EAC1PP	-	-	-
FCS_COP.1/PACE_MAC_EAC1PP	-	-	-
FCS_RND.1/EAC1PP	-	-	-
FCS_CKM.1/CA_EAC1PP	-	-	-
FCS_COP.1/CA_ENC_EAC1PP	-	-	-
FCS_COP.1/SIG_VER_EAC1PP	-	-	-
FCS_COP.1/CA_MAC_EAC1PP	-	-	-
FCS_CKM.1/CA2	X	X	X
FCS_CKM.1/RI	-	X	-
FCS_CKM.1/AA	-	-	-
FCS_COP.1/AA	-	-	-
FCS_CKM.1/CAM	-	-	-
FCS_COP.1/CAM	-	-	-
FCS_CKM.1/SSCDPP	-	-	X
FCS_COP.1/SSCDPP	-	-	X
FIA_AFL.1/Suspend_PIN_EAC2PP	X	X	X
FIA_AFL.1/Block_PIN_EAC2PP	X	X	X
FIA_API.1/CA_EAC2PP	X	X	X
FIA_API.1/RI_EAC2PP	-	X	-
FIA_UID.1/PACE_EAC2PP	X	X	X
FIA_UID.1/EAC2_Terminal_EAC2PP	X	X	X
FIA_UAU.1/PACE_EAC2PP	X	X	X
FIA_UAU.1/EAC2_Terminal_EAC2PP	X	X	X
FIA_UAU.4/PACE_EAC2PP	X	X	X
FIA_UAU.5/PACE_EAC2PP	X	X	X
FIA_UAU.6/CA_EAC2PP	X	X	X
FIA_AFL.1/PACE_EAC2PP	X	X	X
FIA_UAU.6/PACE_EAC2PP	X	X	X
FIA_UID.1/PACE_EAC1PP	-	-	-
FIA_UAU.1/PACE_EAC1PP	-	-	-
FIA_UAU.4/PACE_EAC1PP	-	-	-
FIA_UAU.5/PACE_EAC1PP	-	-	-

FIA_UAU.6/PACE_EAC1PP	-	-	-
FIA_UAU.6/EAC_EAC1PP	-	-	-
FIA_API.1/EAC1PP	-	-	-
FIA_API.1/PACE_CAM	-	-	-
FIA_API.1/AA	-	-	-
FIA_AFL.1/PACE_EAC1PP	-	-	-
FIA_UID.1/SSCDPP	-	-	X
FIA_AFL.1/SSCDPP	-	-	X
FIA_UAU.1/SSCDPP	-	-	X
FDP_ACC.1/TRM_EAC2PP	X	X	X
FDP_ACF.1/TRM	X	X	X
FDP_RIP.1/EAC2PP	X	X	X
FDP_UCT.1/TRM_EAC2PP	X	X	X
FDP_UIT.1/TRM_EAC2PP	X	X	X
FDP_ACC.1/TRM_EAC1PP	-	-	-
FDP_RIP.1/EAC1PP	-	-	-
FDP_UCT.1/TRM_EAC1PP	-	-	-
FDP_UIT.1/TRM_EAC1PP	-	-	-
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
FTP_ITC.1/PACE_EAC2PP	X	X	X
FTP_ITC.1/CA_EAC2PP	X	X	X
FTP_ITC.1/PACE_EAC1PP	-	-	-
FAU_SAS.1/EAC2PP	X	X	X
FAU_SAS.1/EAC1PP	-	-	-
FMT_MTD.1/CVCA_INI_EAC2PP	X	X	X
FMT_MTD.1/CVCA_UPD_EAC2PP	X	X	X
FMT_SMF.1/EAC2PP	X	X	-
FMT_SMR.1	X	X	X
FMT_MTD.1/DATE_EAC2PP	X	X	X
FMT_MTD.1/PA_EAC2PP	X	X	X
FMT_MTD.1/SK_PICC_EAC2PP	X	X	X
FMT_MTD.1/KEY_READ_EAC2PP	X	X	-
FMT_MTD.1/Initialize_PIN_EAC2PP	X	X	-
FMT_MTD.1/Change_PIN_EAC2PP	X	X	
FMT_MTD.1/Resume_PIN_EAC2PP	X	X	
FMT_MTD.1/Unblock_PIN_EAC2PP	X	X	
FMT_MTD.1/Activate_PIN_EAC2PP	X	X	
FMT_MTD.3/EAC2PP	X	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/SignatorySSCDPP	-	-	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/EAC2PP	X	X	X
FMT_LIM.2/EAC2PP	X	X	X
FMT_MTD.1/INI_ENA_EAC2PP	X	X	X
FMT_MTD.1/INI_DIS_EAC2PP	X	X	X
FMT_SMF.1/EAC1PP	-	-	-
FMT_LIM.1/EAC1PP	-	-	-
FMT_LIM.2/EAC1PP	-	-	-
FMT_MTD.1/INI_ENA_EAC1PP	-		-
FMT_MTD.1/INI_DIS_EAC1PP	-	-	-
FMT_MTD.1/CVCA_INI_EAC1PP	-	-	-
FMT_MTD.1/CVCA_UPD_EAC1PP	-	-	-
FMT_MTD.1/DATE_EAC1PP	-	-	-
FMT_MTD.1/CAPK_EAC1PP	-	-	-
FMT_MTD.1/PA_EAC1PP	-	-	-
FMT_MTD.1/KEY_READ_EAC1PP	-	-	-
FMT_MTD.3/EAC1PP	-	-	-
FMT_LIM.1/Loader	-	X	X
FMT_LIM.2/Loader	-	X	X
FMT_MTD.1/AA_Private_Key	-	-	-
FPT_EMS.1/EAC2PP	X	X	X
FPT_FLS.1/EAC2PP	X	X	X
FPT_TST.1/EAC2PP	X	X	X
FPT_PHP.3/EAC2PP	X	X	X
FPT_TST.1/EAC1PP	-	-	
FPT_FLS.1/EAC1PP	-	-	
FPT_PHP.3/EAC1PP	-	-	
FPT_EMS.1/EAC1PP	-	-	
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

1.4.5.3. Identity Card with EU-compliant MRTD Application

Passwords

- MRZ [16]
- CAN [16]
- PIN [17]
- PUK [17]

While it is technically possible to grant access to the electronic signature functionality by inputting only CAN, this technical option is not allowed in this ST. This is due to the fact that solely the signatory – which is here the Electronic Document Holder – shall be able to generate an electronic signature on his own behalf.

Authentication Procedure

This configuration requires implementation at the following Authentication Procedure for access to non-sensitive user data of the ePassport Application:

- Advanded Inspection Procedure [16]

This configuration requires implementation ot the following Authentication Procedure for access any further User Data stored on the TOE:

- General Authentication Procedure [17]

Applications

- ePassport Application
- eID Application
- eSign Application

Protocols

- PACE (Generic Mapping, Integrated Mapping and Chip Authentication Mapping) [9] [16] and [17]
- Active Authentication [7] (optionally)
- EAC1 [16]
  - Terminal Authentication version 1 [16]
  - Chip Authentication version 1 [16]
- EAC2 [17]
  - Terminal Authentication version 2 [17]
  - Chip Authentication version 2 [17]
- Restricted Identification [17]

Data Groups

According to [17].

Data types in Table 5 Terminals and access control in Identity Card with EU-compliant MRTD Application:

- Common user data: All DG, which require only BAC/PACE protocol in ePassport;
- EAC1 protected data: All DG,which require EAC1 protocol in ePassport;
- EAC2 protected data: All DG in eID and eSign application.

532 The authorization level of EAC1 and EAC2 terminals are determined by the effective
533 authorization calculated by from the certificate chain.

534 **Terminals and access control**

Data types	PACE terminal	EAC1 terminal	EAC2 terminal
Common user data	X	X	X
EAC1 protected data	-	X	-
EAC2 protected data	-	-	X

535 Table 5 Terminals and access control in Identity Card with EU-compliant MRTD Application

536

TOE SFR / Application	ePassport	eID	eSign
FCS_CKM.1/DH_PACE_EAC2PP	-	X	X
FCS_COP.1/SHA_EAC2PP	-	X	X
FCS_COP.1/SIG_VER_EAC2PP	-	X	X
FCS_COP.1/PACE_ENC_EAC2PP	-	X	X
FCS_COP.1/PACE_MAC_EAC2PP	-	X	X
FCS_CKM.4/EAC2PP	-	X	X
FCS_RND.1/EAC2PP	-	X	X
FCS_CKM.1/DH_PACE_EAC1PP	X	-	-
FCS_CKM.4/EAC1PP	X	-	-
FCS_COP.1/PACE_ENC_EAC1PP	X	-	-
FCS_COP.1/PACE_MAC_EAC1PP	X	-	-
FCS_RND.1/EAC1PP	X	-	-
FCS_CKM.1/CA_EAC1PP	-	-	-
FCS_COP.1/CA_ENC_EAC1PP	-	-	-
FCS_COP.1/SIG_VER_EAC1PP	X	-	-
FCS_COP.1/CA_MAC_EAC1PP	X	-	-
FCS_CKM.1/CA2	-	X	X
FCS_CKM.1/RI	-	X	-
FCS_CKM.1/AA	X	-	-
FCS_COP.1/AA	X	-	-
FCS_CKM.1/CAM	X	-	-
FCS_COP.1/CAM	X	-	-
FCS_CKM.1/SSCDPP	-	-	X
FCS_COP.1/SSCDPP	-	-	X
FIA_AFL.1/Suspend_PIN_EAC2PP	X	X	X
FIA_AFL.1/Block_PIN_EAC2PP	X	X	X
FIA_API.1/CA_EAC2PP	-	X	X
FIA_API.1/RI_EAC2PP	-	X	-
FIA_UID.1/PACE_EAC2PP	-	X	X
FIA_UID.1/EAC2_Terminal_EAC2PP	-	X	X
FIA_UAU.1/PACE_EAC2PP	-	X	X
FIA_UAU.1/EAC2_Terminal_EAC2PP	-	X	X

FIA_UAU.4/PACE_EAC2PP	-	X	X
FIA_UAU.5/PACE_EAC2PP	-	X	X
FIA_UAU.6/CA_EAC2PP	-	X	X
FIA_AFL.1/PACE_EAC2PP	-	X	X
FIA_UAU.6/PACE_EAC2PP	-	X	X
FIA_UID.1/PACE_EAC1PP	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_API.1/PACE_CAM	X	-	-
FIA_API.1/AA	X	-	-
FIA_AFL.1/PACE_EAC1PP	X	-	-
FIA_UID.1/SSCDPP	-	-	X
FIA_AFL.1/SSCDPP	-	-	X
FIA_UAU.1/SSCDPP	-	-	X
FDP_ACC.1/TRM_EAC2PP	-	X	X
FDP_ACF.1/TRM	X	X	X
FDP_RIP.1/EAC2PP	-	X	X
FDP_UCT.1/TRM_EAC2PP	-	X	X
FDP_UIT.1/TRM_EAC2PP	-	X	X
FDP_ACC.1/TRM_EAC1PP	X	-	-
FDP_RIP.1/EAC1PP	X	-	-
FDP_UCT.1/TRM_EAC1PP	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
FTP_ITC.1/PACE_EAC2PP	-	X	X
FTP_ITC.1/CA_EAC2PP	-	X	X
FTP_ITC.1/PACE_EAC1PP	X	-	-
FAU_SAS.1/EAC2PP	-	X	X
FAU_SAS.1/EAC1PP	X	-	-
FMT_MTD.1/CVCA_INI_EAC2PP	-	X	X
FMT_MTD.1/CVCA_UPD_EAC2PP	-	X	X
FMT_SMF.1/EAC2PP	-	X	-
FMT_SMR.1	X	X	X
FMT_MTD.1/DATE_EAC2PP	-	X	X
FMT_MTD.1/PA_EAC2PP	-	X	X
FMT_MTD.1/SK_PICC_EAC2PP	-	X	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_SMR.1/SSCDPP	-	-	X
FMT_SMF.1/SSCDPP	-	-	X
FMT_MOF.1/SSCDPP	-	-	X
FMT_MSA.1/Admin_SSCDPP	-	-	X
FMT_MSA.1/SignatorySSCDPP	-	-	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/EAC2PP	-	X	X
FMT_LIM.2/EAC2PP	-	X	X
FMT_MTD.1/INI_ENA_EAC2PP	-	X	X
FMT_MTD.1/INI_DIS_EAC2PP	-	X	X
FMT_SMF.1/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	-	-	-
FMT_LIM.1/Loader	X	X	X
FMT_LIM.2/Loader	X	X	X
FMT_MTD.1/AA_Private_Key	X	-	-
FPT_EMS.1/EAC2PP	-	X	X
FPT_FLS.1/EAC2PP	-	X	X
FPT_TST.1/EAC2PP	-	X	X
FPT_PHP.3/EAC2PP	-	X	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

5. Application note (from the ST author)

Taking into consideration the [20] specifies authentication and communication protocols that have to be used for the eSign application for the TOE, all the EAC2 relevant SFR are listed to the eSign application as well. These SFRs contribute to secure Signature Verification Data (SVD) export, Data To Be Signed (DTBS) import, and Verification Authentication Data (VAD) import functionality.

2. Conformance Claims

2.1. CC Conformance Claim

This ST claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017, [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017, [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017, [3]

as follows

Part 2 extended,

Part 3 conformant.

The

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

has to be taken into account.

2.2. PP Claim

This ST claims **strict conformance** to the following protection profile:

Title:	**Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP] [20]**
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
CC version:	3.1 (Revision 3.4)
Assurance Level:	EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.
General Status:	Final
Version number:	1.01
Registration:	BSI-CC-PP-0087

Keywords:	ICAO, PACE, EAC, Extended Access Control, ID-Card, electronic document, smart card, TR-03110

Since the [20] claims strict conformance to [5], [6] and [14], this ST also claims **strict conformance** to

Title:	**Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE (EAC PP) [5]**
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik
CC Version:	3.1 (revision 3)
Assurance Level:	EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
General Status:	Final
Version number:	version 1.3.2
Registration:	BSI-CC-PP-0056-V2-2012
Keywords:	ICAO, Machine Readable Travel Document, Extended Access Control, PACE, Supplemental Access Control (SAC)

Title:	**Common Criteria Protection Profile Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110 [6]**
Editor/Sponsor:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
CC Version:	3.1 (Revision 4)
Assurance Level:	EAL4 augmented ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.
General Status:	final
Version Number:	Version 1.01
Registration:	BSI-CC-PP-0086
Keywords:	EAC2, eID-Application, eID-Card, PACE

Title:	**Protection profiles for Secure signature creation device — Part 2: Device with key generation**
Author:	CEN / CENELEC (TC224/WG17)
CC Version:	3.1 (Revision 3)
Assurance Level:	EAL4 augmented with AVA_VAN.5
Version Number:	Version 2.0.1

Registration:	BSI-CC-PP-0059-2009-MA-01
Keywords:	secure signature-creation device, electronic signature, digital signature

6. Application note (taken from [20] Application note 7)

This conformance claim covers the part of the security policy for the eSign application of the TOE corresponding to the security policy defined in [14], and hence is applicable, if the eSign application is operational. In addition to [14], the current ST specifies authentication and communication protocols (at least PACE) that have to be used for the eSign application of the TOE. These protocols contribute to secure Signature Verification Data (SVD) export, Data To Be Signed (DTBS) import, and Verification Authentication Data (VAD) import functionality.

Since [5] and [6] claim strict conformance to [13], this ST implicitly also claims **strict conformance** to

Title:	**Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) [13]**
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik
CC Version:	3.1 (revision 4)
Assurance Level:	EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
General Status:	Final
Version number:	Version 1.01
Registration:	BSI-CC-PP-0068-V2-2011-MA-01
Keywords:	ePassport, travel document, ICAO, PACE, Standard Inspection Procedure, Supplemental Access Control (SAC)

However since [5] and [6] already claim strict conformance to [13], this implicit conformance claim is formally mostly ignored within this ST for the sake of presentation; but if necessary to yield a better overview however, references to [13] are given or the relation with [13] is explained.

2.3.Package Claim

The current ST is conformant to the following packages:

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

2.4.Conformance Rationale

This ST conforms to the PPs [20], [5], [6] and [14]. This implies for this ST:

1. The TOE type of this ST is the same 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 [16] and [17], and additionally representing a combination of hardware and software configured to securely create, use and manage signature-creation data , for the eSign application.
2. 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.
   The current ST extended the OSP **P.Terminal** because of the optional Active Authentication function of TOE.
3. The security objectives for the TOE in this ST include all the security objectives for the TOE of the claimed PPs. This objective does not weaken the security objectives of the claimed PPs.
   In addition, the OT.Chip_Auth_Proof_PACE_CAM security objective is defined in the ST because of the Chip Authentication mapping and OT.Chip_Auth_Proof_AA because of the Active Authentication protocol.
4. The security objectives for the operational environment in this ST include all security objectives for the operational environment of the claimed PPs.
   In addition the OE.Auth_Key_AA and OE.Exam_Electronic_Document_AA security objectives are defined in the ST because of the Active Authentication protocol. These additions were necessary because none of the original security objectives for the TOE or OSPs do not concern the obligations of States or Organization in connection with Active Authentication protocol.
5. Those SFR, which are refined in order to ensure the unified terminology usage, are not detailed in the following.
   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 [20]:
   The SFR FIA_UAU.1/SSCDPP is redefined from [14] by additional assignments. Note that this does not violate strict conformance to [14].
   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 following SFRs were iterated from FCS_CKM.1, FCS_COP.1 and FIA_API.1 to the ST because of PACE-CAM:

- FCS_CKM.1/CAM
- FCS_COP.1/CAM
- FIA_API.1/PACE_CAM

The following SFR was extended to the ST because of PACE-CAM:

- FPT_EMS.1/EAC1PP

The following SFRs were refined to the ST because of PACE-CAM:

- FIA_UID.1/PACE_EAC1PP
- FIA_UAU.5/PACE_EAC1PP

The following SFRs were iterated from FCS_CKM.1, FCS_COP.1, FIA_API.1 and FMT_MTD.1 to the ST because of Active Authentication protocol:

- FCS_CKM.1/AA
- FCS_COP.1/AA
- FIA_API.1/AA
- FMT_MTD.1/AA_Private_Key

The following SFRs was extended to the ST because of Active Authentication protocol:

- FIA_UAU.1/PACE_EAC1PP
- FPT_EMS.1/EAC1PP

The following SFRs were refined to the ST because of Active Authentication protocol:

- FIA_UAU.4/PACE_EAC1PP
- FMT_MTD.1/KEY_READ_EAC1PP

The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip Authentication version 2 and Restricted Identification key pair(s) generation on the TOE as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were refined to emphasize the purpose of the SFRs:

- FCS_CKM.1/CA2
- FCS_CKM.1/RI

The following SFR is refined because the electronic document manufacturer may generate or load the private keys:

- FMT_MTD.1/SK_PICC_EAC2PP

The following SFR is slightly refined in order not to confuse Chip Authentication 1 with Chip Authentication 2:

- FDP_RIP.1/EAC2PP

These additional SFRs do not affect the strict conformance. All assignments and selections of the security functional requirements are defined in the [6] section 6.1 and in this ST Security Functional Requirements.

The extension of the OSP **P.Terminal** do not affect the strict conformance because it do not modify the original requirements only added new requirements concern the Active Authentication protocol.

The SARs specified in this ST are the same as specified in the claimed PPs or extend them.

2.5.Statement of Compatibility

2.5.1. Security Functionalities

The following table contains the security functionalities of the [23] and of current ST, showing which Functionality correspond to the [23] and which has no correspondence. This statement is compliant to the requirements of [25].

A classification of SFs of the [23] has been made. Each TSF has been classified as 'relevant' or 'not relevant' for current ST.

Platform Security Functionality	Corresponding TOE Security Functionality	Relevant or not relevant	Remarks
SF.JCVM	TSF.Platform	Relevant	Java Card Virtual Machine
SF.CONFIG	TSF.Platform	Relevant	Configuration Management
SF.OPEN	TSF.AccessControl TSF.Authenticate TSF.Platform	Relevant	Card Content Management
SF.CRYPTO	TSF.AppletParametersSign TSF.Authenticate TSF.CryptoKey TSF.Platform	Relevant	Cryptographic Functionality
SF.RNG	TSF.CryptoKey TSF.Platform	Relevant	Random Number Generator
SF.DATA_STORAGE	TSF.AccessControl TSF.AppletParametersSign TSF.CryptoKey TSF.Platform	Relevant	Secure Data Storage

Platform Security Functionality	Corresponding TOE Security Functionality	Relevant or not relevant	Remarks
SF.PUF	-	Relevant	User Data Protection using PUF
SF.EXT_MEM	-	Not relevant	External Memory
SF.OM	TSF.Platform	Relevant	Java Object Management
SF.MM	-	Not relevant	Memory Management
SF.PIN	TSF.AppletParametersSign TSF.Authenticate	Relevant	PIN Management
SF.PERS_MEM	TSF.Platform	Relevant	Persistent Memory Management
SF.SENS_RES	-	Not relevant	Sensitive Result
SF.EDC	TSF.Platform	Relevant	Error Detection Code API
SF.HW_EXC	TSF.Platform	Relevant	Hardware Exception Handling
SF.RM	-	Not relevant	Restricted Mode
SF.PID	-	Not relevant	Platform Identification
SF.SMG_NSC	TSF.Platform	Relevant	No Side-Channel
SF.ACC_SBX	-	Not relevant	Secure Box
SF.MOD_INVOC	-	Not relevant	Module Invocation

Table 6 Classification of Platform-TSFs

All the above SFs of [23], which are indicated as relevant are relevant for this ST.

2.5.2. OSPs

P.Card_PKI, P.Trustworthy_PKI, P.Terminal, P.Sensitive_Data, P.Personalisation, P.EAC2_Terminal, P.RestrictedIdentity and P.Terminal_PKI are not applicable to the Platform and therefore not mappable for [23].

The OSP.VERIFICATION, OSP.PROCESS-TOE, OSP.KEY-CHANGE are covered by the ALC class, furthermore P.Manufact, P.Pre-Operational and P.Lim_Block_Loader correspond to these OSPs.

OSP.SECURE-BOX and OSP.SECURITY-DOMAINS do not deal with any additional security components.

2.5.3. Security Objectives

These objectives from [23] can be mapped to this ST's objectives as shown in the following table, so they are relevant.

Objective from the Platform ST	Objective from this ST
OT.ALARM	OT.SCD_Secrecy

	OT.Tamper_Resistance
	OT.Data_Integrity
	OT.Prot_Inf_Leak
	OT.Prot_Phys-Tamper
OT.CARD-CONFIGURATION	OT.Prot_Abuse-Func
OT.CARD-MANAGEMENT	OT.AC_Pers
	OT.AC_Pers
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Identification
	OT.Sens_Data_Conf
	OT.AC_PERS_EAC2
OT.CIPHER	OT.Lifecycle_Security
	OT.SCD_Unique
	OT.SCD_SVD_Corresp
	OT.SCD_Secrecy
	OT.AC_Pers
	OT.Active_Auth_Proof
	OT.Chip_Auth_Proof
	OT.Chip_Auth_Proof_PACE_CAM
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Sens_Data_Conf
	OT.CA2
OT.COMM_AUTH	OT.Lifecycle_Security
	OT.Sig_Secure
	OT.TOE_QSCD_Auth
	OT.AC_Pers
	OT.Chip_Auth_Proof
	OT.Chip_Auth_Proof_PACE_CAM
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Identification
	OT.Sens_Data_Conf
	OT.Tracing
	OT.Sens_Data_EAC2
OT.COMM_CONFIDENTIALITY	OT.Lifecycle_Security
	OT.Sig_Secure
	OT.TOE_QSCD_Auth
	OT.TOE_TC_SVD_Exp
	OT.AC_Pers
	OT.Chip_Auth_Proof
	OT.Chip_Auth_Proof_PACE_CAM
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity

	OT.Identification
	OT.Sens_Data_Conf
	OT.Tracing
	OT.RI_EAC2
	OT.Sens_Data_EAC2
OT.COMM_INTEGRITY	OT.Lifecycle_Security
	OT.AC_Pers
	OT.Chip_Auth_Proof
	OT.Chip_Auth_Proof_PACE_CAM
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Identification
	OT.Sens_Data_Conf
	OT.Tracing
	OT.Sig_Secure
	OT.TOE_QSCD_Auth
	OT.TOE_TC_SVD_Exp
	OT.RI_EAC2
	OT.Sens_Data_EAC2
OT.COMM_AUTH	OT.AC_Pers
	OT.Chip_Auth_Proof
	OT.Chip_Auth_Proof_PACE_CAM
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Identification
	OT.Sens_Data_Conf
	OT.Tracing
	OT.RI_EAC2
	OT.AC_PERS_EAC2
	OT.Sens_Data_EAC2
OT.DOMAIN-RIGHTS	OT.AC_Pers
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Identification
	OT.Sens_Data_Conf
OT.GLOBAL_ARRAYS_CONFID	OT.SCD_Secrecy
	OT.Sigy_SigF
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Sens_Data_EAC2
OT.IDENTIFICATION	OT.AC_Pers
	OT.Identification
OT.KEY-MNGT	OT.Lifecycle_Security
	OT.SCD_Unique
	OT.SCD_SVD_Corresp

	OT.SCD_Secrecy
	OT.Sig_Secure
	OT.TOE_QSCD_Auth
	OT.TOE_TC_SVD_Exp
	OT.Sigy_SigF
	OT.AC_Pers
	OT.Chip_Auth_Proof
	OT.Chip_Auth_Proof_PACE_CAM
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Prot_Inf_Leak
	OT.Prot_Malfunction
	OT.Sens_Data_Conf
	OT.CA2
	OT.RI_EAC2
	OT.Sens_Data_EAC2
OT.OPERATE	OT.SCD_Secrecy
	OT.Data_Integrity
	OT.Prot_Inf_Leak
	OT.Prot_Malfunction
	OT.Prot_Phys-Tamper
OT.PIN-MNGT	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Prot_Inf_Leak
	OT.Prot_Malfunction
	OT.Sens_Data_EAC2
OT.REALLOCATION	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Sens_Data_EAC2
OT.RESOURCES	OT.Data_Integrity
	OT.Prot_Inf_Leak
	OT.Prot_Phys-Tamper
OT.RND	OT.AC_Pers
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Sens_Data_Conf
	OT.Sens_Data_EAC2
OT.RNG	OT.AC_Pers
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Sens_Data_Conf
	OT.Sens_Data_EAC2
OT.SCP.IC	OT.AC_Pers
	OT.Data_Integrity
	OT.Prot_Inf_Leak

	OT.Prot_Phys-Tamper
OT.SCP.RECOVERY	OT.Data_Integrity
	OT.Prot_Inf_Leak
	OT.Prot_Phys-Tamper
OT.SCP.SUPPORT	OT.AC_Pers
	OT.Chip_Auth_Proof
	OT.Chip_Auth_Proof_PACE_CAM
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Sens_Data_Conf
	OT.Tracing
	OT.CA2
	OT.RI_EAC2
	OT.Sens_Data_EAC2
OT.SID_MODULE	OT.Prot_Inf_Leak
	OT.Prot_Malfunction
OT.TRANSACTION	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Sens_Data_EAC2

Table 7 Mapping of security objectives for the TOE

The following objectives of [23] are not relevant for or cannot be mapped to the TOE of this ST:

- **OT.SID**
- **OT.APPLI-AUTH**
- **OT.ATTACK-COUNTER**
- **OT.EXT-MEM**
- **OT.FIREWALL**
- **OT.Global_ARRAYS_INTEG**
- **OT.NATIVE**
- **OT.OBJ-DELETION**
- **OT.RESTRICTED-MODE**
- **OT.SEC_BOX_FW**
- **OT.SENSITIVE_RESULT_INTEG**

cannot be mapped because these are out of scope.

The objectives for the operational environment can be mapped as follows:

Objective from the Platform-ST	Classification of OE	Objective from this ST
OE.APPLET	CfPOE	Covered by ALC class

OE.PROCESS_SEC_IC	CfPOE	Covered by the Platform's certification and ALC class
OE.VERIFICATION	CfPOE	Covered by ALC class
OE.CODE-EVIDENCE	CfPOE	Covered by ALC class
OE.USE_DIAG	SgOE	Covered by OE.Terminal, OE.Exam_Travel_Document, OE.Prot_Logical_Travel_Document and OE.SSCD_Prov_Service
OE.USE_KEYS	SgOE	Covered by OE.Terminal, OE.Exam_Travel_Document, OE.Prot_Logical_Travel_Document, OE.Terminal_Authentication and OE.HID_VAD
OE.APPS-PROVIDER	CfPOE	Covered by ALC class
OE.VERIFICATION-AUTHORITY	CfPOE	Covered by ALC class
OE.KEY-CHANGE	CfPOE	Covered by ALC class
OE.SECURITY-DOMAINS	CfPOE	Covered by ALC class

746 There is no conflict between security objectives of this ST and the [23].

747 2.5.4. Security Requirements

748 The Security Requirements of the Platform ST can be mapped as follows:

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
FAU_ARP.1	FPT_PHP.3/EAC2PP FPT_PHP.3/EAC1PP FPT_PHP.3/SSCDPP	RP_SFR-MECH	FAU_ARP.1 facilitate to protect the TOE as required by these SFRs./SSCD
FAU_SAS.1[SCP]	FAU_SAS.1/EAC2PP FAU_SAS.1/EAC1PP	RP_SFR-MECH	FAU_SAS.1[SCP] covers these SFRs.
FCO_NRO.2[SC]	-	IP_SFR	-
FCS_CKM.1t	-	IP_SFR	-
FCS_COP.1	FCS_CKM.1/DH_PACE_EAC2PP FCS_CKM.1/DH_PACE_EAC1PP	RP_SFR-SERV	FCS_COP.1.1[ECDHPACEKeyAgreement] is applied for key agreement during the PACE and CA2 protocols. FCS_COP1.1[SHA] is applied for session key derivation during PACE, protocols.

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
	FCS_CKM.1/CAM	RP_SFR-SERV	FCS_COP.1.1[ECDHPACEKeyAgreement] is applied for key agreement during the PACE-CAM.
	FCS_CKM.1/CA2	RP_SFR-SERV	FCS_CKM.1.1 is applied for generation chip authentication key(s) pair on the TOE:
	FCS_CKM.1/RI	RP_SFR-SERV	FCS_CKM.1.1 is applied for generation chip restricted identification key pair(s) on the TOE:
	FCS_CKM.1/AA	RP_SFR-SERV	FCS_CKM.1.1 is applied for generation chip active authentication key pair on the TOE:
	FCS_CKM.1/SSCDPP	RP_SFR-SERV	FCS_CKM.1.1 is applied for generation chip SCD/SVD key pair on the TOE:
	FCS_COP.1/PACE_ENC_EAC2PP	RP_SFR-SERV	FCS_COP1.1[AES] is applied for nonce encryption during the PACE protocol. FCS_COP1.1[AES] is applied for encryption and decryption during secure messaging (PACE)
	FCS_COP.1/PACE_ENC_EAC1PP	RP_SFR-SERV	FCS_COP1.1[AES] or FCS_COP.1[TripleDES] is applied for nonce encryption during the PACE-CAM protocol. FCS_COP1.1[AES] or FCS_COP.1[TripleDES] is applied for encryption and decryption during secure messaging (PACE).
	FCS_COP.1/SHA_EAC2PP	RP_SFR-SERV	FCS_COP1.1[SHA] is applied for session key derivation during CA2 and ephemeral key compression (CA2 and TA2).
	FCS_COP.1/CAM	RP_SFR-SERV	FCS_COP.1.1[AES] is applied for message encryption of Chip Authentication Data.
	FCS_CKM.1/CA_EAC1PP	RP_SFR-SERV	FCS_COP.1.1[ECDHPACEKeyAgreement] is applied for key agreement related to CA1 FCS_COP1.1[SHA] is applied for session key derivation during CA1.
	FCS_COP.1/SIG_VER_EAC2PP	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] orFCS_COP.1.1[ECSignature]

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
			for digital signature verification related to TA2.
	FCS_COP.1/PACE_MAC_EAC2PP	RP_SFR-SERV	FCS_COP.1.1[AESMAC] is applied to generate and verify the message authentication codes.
	FCS_COP.1/PACE_MAC_EAC1PP	RP_SFR-SERV	FCS_COP.1.1[DESMAC] or FCS_COP.1.1[AESMAC] is applied to generate and verify the message authentication codes.
	FCS_COP.1/CA_ENC_EAC1PP	RP_SFR-SERV	FCS_COP.1[TripleDES] or FCS_COP1.1[AES] is applied for encryption and decryption during secure messaging (CA1)
	FCS_COP.1/CA_MAC_EAC1PP	RP_SFR-SERV	FCS_COP.1.1[DESMAC] or FCS_COP.1.1[AESMAC] is applied to generate and verify the message authentication codes (CA1)
	FCS_COP.1/SIG_VER_EAC1PP	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] orFCS_COP.1.1[ECSignature] for digital signature verification related to TA1.
	FCS_COP.1/AA	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] orFCS_COP.1.1[ECSignature] for digital signature generation related to Active Authentication.
	FCS_COP.1/SSCDPP	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] or FCS_COP.1.1[ECSignature] for digital signature creation.
	FIA_API.1/CA_EAC2PP	RP_SFR-SERV	FCS_COP.1 fAESMAC] is applied for generating the authentication token.
	FIA_API.1/RI_EAC2PP	RP_SFR-SERV	FCS_COP.1.1[ECDHPACEKeyAgreement] is applied for key agreement related to RI FCS_COP1.1[SHA] is applied for restricted identification.
	FIA_UAU.5/PACE_EAC2PP	RP_SFR-SERV	FCS_COP1.1[AESMAC] is applied during PACE secure messaging the verify the message authentication codes. FCS_COP1.1[AESMAC] is applied during CA secure messaging to verify the

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
			message authentication codes. FCS_COP1.1[AESMAC] is applied during secure messaging to verify the message authentication codes. FCS_COP1.1[SHA] is applied for public key compression (in case DH).
	FIA_UAU.5/PACE_EAC1PP	RP_SFR-SERV	FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during PACE secure messaging the verify the message authentication codes. FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during CA secure messaging to verify the message authentication codes. FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during secure messaging (based on Personalisation Agent Key) to verify the message authentication codes. FCS_COP1.1[SHA] is applied for public key compression (in case DH).
	FIA_UAU.6/PACE_EAC2PP FIA_UAU.6/PACE_EAC1PP	RP_SFR-SERV	FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during PACE secure messaging the verify the message authentication codes
	FIA_UAU.6/EAC_EAC1PP	RP_SFR-SERV	FCS_COP.1.1[AESMAC] o FCS_COP.1[DESMAC] is applied for message authentication code generation and verification related to PACE.
	FIA_UAU.6/CA_EAC2PP	RP_SFR-SERV	FCS_COP.1.1[AESMAC] is applied for message authentication code generation and verification related to CA2.
	FIA_UAU.6/EAC_EAC1PP	RP_SFR-SERV	FCS_COP.1.1[AESMAC] o FCS_COP.1[DESMAC] is applied for message authentication code

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
			generation and verification related to CA1.
	FIA_API.1/EAC1PP	RP_SFR-SERV	FCS_COP1.1[AESMAC] is applied for message authentication code verification related to CA1.
	FIA_API.1/AA	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] or FCS_COP.1.1[ECSignature] is applied for digital signature verification for Active Authentication protocol..
	FIA_API.1/PACE_CAM	RP_SFR-SERV	FCS_COP.1.1[AESMAC] is applied for chip authentication data generation related to PACE-CAM.
	FDP_UCT.1/TRM_EAC1PP	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] or FCS_COP.1.1[ECSignature] is applied for digital signature verification for TA.
	FDP_UIT.1/TRM_EAC1PP	RP_SFR-SERV	FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during PACE secure messaging the verify the message authentication codes. FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during CA secure messaging to verify the message authentication codes. FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during secure messaging (based on Personalisation Agent Key) to verify the message authentication codes. FCS_COP1.1[SHA] is applied for public key compression (in case DH).
	FTP_ITC.1/PACE_EAC2PP	RP_SFR-SERV	FCS_COP.1[AES] and or FCS_COP.1[AESMAC] are applied during secure messaging to protect against disclosure and modification
	FTP_ITC.1/CA_EAC2PP	RP_SFR-SERV	FCS_COP.1[AES] and FCS_COP.1[AESMAC] are applied during secure

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
			messaging to protect against disclosure and modification
	FTP_ITC.1/PACE_EAC1PP	RP_SFR-SERV	FCS_COP.1[TripleDES] or FCS_COP.1[AES] and FCS_COP.1[DESMAC] or FCS_COP.1[AESMAC] are applied during secure messaging to protect against disclosure and modification
	FMT_MTD.3/EAC2PP FMT_MTD.3/EAC1PP	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] or FCS_COP.1.1[ECSignature] is applied for digital signature verification for TA1 and TA2.
FCS_RNG.1	FCS_RND.1/EAC2PP	RP_SFR-SERV	FCS_RNG.1 provides nonce and challenge generation for PACE and TA2.
	FCS_RND.1/EAC1PP	RP_SFR-SERV	FCS_COP.1[TripleDES] or FCS_COP.1[AES] is applied during secure messaging to protect the confidentiality of transmitted and received user data.
	FIA_UAU.4/PACE_EAC2PP	RP_SFR-SERV	FCS_RNG.1 is applied to generate fresh nonce for PACE and TA2
	FIA_UAU.4/PACE_EAC1PP	RP_SFR-SERV	FCS_RNG.1 is applied to generate fresh nonce for PACE, TA1 and Active Authentication.
	FDP_UCT.1/TRM_EAC2PP	RP_SFR-SERV	FCS_COP.1[AESMAC] is applied during secure messaging to protect the integrity of transmitted and received user data.
	FDP_UIT.1/TRM_EAC2PP	RP_SFR-SERV	FCS_COP.1[AES] is applied during secure messaging to protect the confidentiality of transmitted and received user data.
FCS_CKM.4	FCS_CKM.4/EAC2PP	RP_SFR-SERV	FCS_CKM.4 of the Platform matches this SFR..
FCS_RNG.1[HDT]	-	IP_SFR	-
FDP_ACC.2[FIREWALL]	-	IP_SFR	
FDP_ACF.1[FIREWALL]	-	IP_SFR	
FDP_ACC.1[SD]	-	IP_SFR	-
FDP_ACF.1[SD]	-	IP_SFR	
FDP_ACC.2[ADEL]	-	IP_SFR	-

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
FDP_ACF.1[ADEL]	-	IP_SFR	
FDP_ACC.2[RM]	-	IP_SFR	-
FDP_ACC.1[EXT-MEM]	-	IP_SFR	
FDP_ACF.1[EXT-MEM]	-	IP_SFR	-
FDP_ACC.2[SecureBox]	-	IP_SFR	
FDP_ACF.1[SecureBox]	-	IP_SFR	
FDP_ACF.1[RM]	-	IP_SFR	-
FDP_IFC.1[JCVM]	-	IP_SFR	-
FDP_IFC.2[SC]	-	IP_SFR	-
FDP_IFC.2[CFG]	FMT_LIM.1/Loader FMT_LIM.2/Loader FMT_LIM.1/EAC2PP FMT_LIM.2/EAC2PP FMT_LIM.1/EAC1PP FMT_LIM.2/EAC1PP	RP_SFR-MECH	FDP_IFC.2[CFG] applied to protect the TOE in operational phase.
FDP_IFC.1[MODULAR-DESIGN]	-	IP_SFR	
FDP_IFF.1[JCVM]	-	IP_SFR	-
FDP_IFF.1[SC]	FMT_MTD.1/INI_ENA_EAC2PP FMT_MTD.1/INI_DIS_EAC2PP FMT_MTD.1/INI_ENA_EA1PP FMT_MTD.1/INI_DIS_EAC1PP	RP_SFR-MECH	FDP_IFF.1[SC] applied to control the writing of initialization and pre-personalization data as required by these SFRs.
FDP_IFF.1[CFG]	-	IP_SFR	-
FDP_IFF.1[MODULAR-DESIGN]	-	IP_SFR	-
FDP_ITC.2[CCM]	-	IP_SFR	-
FDP_RIP.1[OBJECTS]	-	IP_SFR	-
FDP_RIP.1[ABORT]	-	IP_SFR	-
FDP_RIP.1[APDU]	-	IP_SFR	-
FDP_RIP.1[bArray]	-	IP_SFR	-
FDP_RIP.1[GlobalArray_Refined]	-	IP_SFR	-
FDP_RIP.1[KEYS]	FDP_RIP.1/EAC2PP FDP_RIP.1/EAC1PP FDP_RIP.1/SSCDPP	RP_SFR-MECH	FDP_RIP.1[KEYS] is applied to destroy the secure message session keys, the PACE

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
			ephemeral private key and SCD.
FDP_RIP.1[TRANSIENT]	-	IP_SFR	-
FDP_RIP.1[ADEL]	-	IP_SFR	-
FDP_RIP.1[ODEL]	-	IP_SFR	-
FDP_ROL.1[FIREWALL]	-	IP_SFR	-
FDP_ROL.1[CCM]	-	IP_SFR	-
FDP_SDI.2[DATA]	FPT_TST.1/EAC2PP FPT_TST.1/EAC1PP FPT_TST.1/SSCDPP	RP_SFR-MECH	FDP_SDI.2[DATA] checks the integrity of TSF data.
	FDP_SDI.2/DTBS_SSCDPP	RP_SFR-MECH	FDP_SDI.2[DATA] is applied to protect DTBS against integrity errors.
	FDP_SDI.2/Persistent_SSCDPP	RP_SFR-MECH	FDP_SDI.2[DATA] is applied to protect SCD against integrity errors.
FDP_SDI.2[SENSITIVE_RESULT]	-	IP_SFR	-
FDP_UIT.1[CCM]	-	IP_SFR	-
FIA_AFL.1[PIN]	FIA_AFL.1/PACE_EAC2PP	IP_SFR	FIA_AFL.1[PIN] is applied for PIN management.
	FIA_AFL.1/SSCDPP	IP_SFR	FIA_AFL.1[PIN] is applied for PIN management.
FIA_ATD.1[AID]	-	IP_SFR	-
FIA_ATD.1[MODULAR-DESIGN]	-	IP_SFR	-
FIA_UID.1[SC]	FIA_UID.1/PACE_EAC2PP FIA_UID.1/EAC2_Terminal_EAC2PP FIA_UID.1/PACE_EAC1PP	RP_SFR-MECH	FIA_UID.1[SC] handled the identifier data of the TOE.
FIA_UID.1[CFG]	-	IP_SFR	-
FIA_UID.1[RM]	-	IP_SFR	-
FIA_UID.2[AID]	-	IP_SFR	-
FIA_UID.1[MODULAR-DESIGN]	-	IP_SFR	-
FIA_USB.1[AID]	-	IP_SFR	-
FIA_USB.1[MODULAR-DESIGN]	-	IP_SFR	-
FIA_UAU.1[RM]	-	IP_SFR	
FIA_UAU.1[SC]	FIA_UAU.1/EAC2_Terminal_EAC2PP FIA_UAU.1/PACE_EAC2PP FIA_UAU.1/PACE_EAC1PP	RP_SFR-MECH	FIA_UAU.1[SC] handled the identifier data of the TOE.

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
FIA_UAU.4[SC]	-	IP_SFR	-
FMT_MSA.1[JCRE]	-	IP_SFR	-
FMT_MSA.1[JCVM]	-	IP_SFR	-
FMT_MSA.1[ADEL]	-	IP_SFR	-
FMT_MSA.1[SC]	-	IP_SFR	-
FMT_MSA.1[EXT-MEM]	-	IP_SFR	-
FMT_MSA.1[SecureBox]	-	IP_SFR	-
FMT_MSA.1[CFG]	-	IP_SFR	-
FMT_MSA.1[SD]	-	IP_SFR	-
FMT_MSA.1[RM]	-	IP_SFR	-
FMT_MSA.1[MODULAR-DESIGN]	-	IP_SFR	-
FMT_MSA.2[FIREWALL-JCVM]	-	IP_SFR	-
FMT_MSA.3[FIREWALL]	-	IP_SFR	-
FMT_MSA.3[JCVM]	-	IP_SFR	-
FMT_MSA.3[ADEL]	-	IP_SFR	-
FMT_MSA.3[EXT-MEM]	-	IP_SFR	-
FMT_MSA.3[SecureBox]	-	IP_SFR	-
FMT_MSA.3[CFG]	-	IP_SFR	-
FMT_MSA.3[SD]	-	IP_SFR	-
FMT_MSA.3[SC]	-	IP_SFR	-
FMT_MSA.3[RM]	-	IP_SFR	-
FMT_MSA.3[MODULAR-DESIGN]	-	IP_SFR	-
FMT_MTD.1[JCRE]	-	IP_SFR	-
FMT_MTD.3[JCRE]	-	IP_SFR	-
FMT_SMF.1	-	IP_SFR	-
FMT_SMF.1[ADEL]	-	IP_SFR	-
FMT_SMF.1[EXT-MEM]	-	IP_SFR	-
FMT_SMF.1[SecureBox]	-	IP_SFR	-

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
FMT_SMF.1[CFG]	-	IP_SFR	-
FMT_SMF.1[SD]	-	IP_SFR	-
FMT_SMF.1[SC]	-	IP_SFR	-
FMT_SMF.1[RM]	-	IP_SFR	-
FMT_SMF.1[MODULAR-DESIGN]	-	IP_SFR	-
FMT_SMR.1	-	IP_SFR	-
FMT_SMR.1[INSTALLER]	-	IP_SFR	-
FMT_SMR.1[ADEL]	-	IP_SFR	-
FMT_SMR.1[CFG]	-	IP_SFR	-
FMT_SMR.1[SD]	-	IP_SFR	-
FMT_SMR.1[MODULAR-DESIGN]	-	IP_SFR	-
FPR_UNO.1	-	IP_SFR	-
FPT_EMSEC.1	FPT_EMS.1/EAC2PP FPT_EMS.1/EAC1PP FPT_EMS.1/SSCDPP	RP_SFR-MECH	FPT_EMSEC.1 of the Platform matches these SFRs.
FPT_FLS.1	FPT_FLS.1/EAC2PP FPT_FLS.1/EAC1PP FPT_FLS.1/SSCDPP	RP_SFR-MECH	FPT_FLS.1 of the Platform ensures the secure state of the TOE as required by FPT_FLS.1
FPT_FLS.1[INSTALLER]	-	IP_SFR	-
FPT_FLS.1[ADEL]	-	IP_SFR	-
FPT_FLS.1[ODEL]	-	IP_SFR	-
FPT_FLS.1[CCM]	-	IP_SFR	-
FPT_FLS.1[MODULAR-DESIGN]	-	IP_SFR	-
FPT_TDC.1	-	IP_SFR	-
FPT_RCV.3[INSTALLER]	-	IP_SFR	-
FPT_PHP.3	FPT_PHP.3/EAC2PP FPT_PHP.3/EAC1PP FPT_PHP.1/SSCDPP FPT_PHP.3/SSCDPP	RP_SFR-MECH	FPT_PHP.3 of the Platform matches these SFRs.
FTP_ITC.1[SC]	-	IP_SFR	-
ADV_SPM.1	-	IP_SFR	-

749 Table 8 Mapping of Security requirements

750 The FMT_LIM.1/EAC2PP, FMT_LIM.2/EAC2PP, FMT_LIM.1/EAC1PP and FMT_LIM.2/EAC1PP are not covered directly by [23]. As described in [20] the purposes of these SFRs is to prevent misuse of test features of the TOE over the life cycle phases.

According to [23] the Platform consists of the Micro Controller, CryptoLibrary and Operation System, which are certified as well. By the Micro Controller the limited availability and capability of test features are ensured after Manufacturing phase of the TOE. FMT_LIM.1 and FMT_LIM.2 is covered by the following Security Functions of Micro Controller ST: TSF.Control. For details please check: [34]

To sum up the above-mentioned Security Functions of Micro Controller ensure that the test features of TOE cannot be misused.

The Personalization Agent (FMT_SMR.1) may use the GlobalPlatform function of the Platform.

The TOE initialization and pre-personalization (FMT_SMF.1/EAC2PP and FMT_SMF.1/EAC1PP) rely on the Platform functions.

2.5.5. Assurance Requirements

This ST requires EAL 4 according to Common Criteria V3.1 R5 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

The [23] requires EAL 6 according to Common Criteria V3.1 R5 augmented by: ASE_TSS.2 and ALC_FLR.1.

As EAL 6 covers all assurance requirements of EAL 4 all non-augmented parts of this ST will match to the [23] assurance requirements.

2.6. Analysis

Overall there is no conflict between security requirements of this ST and [23].

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 [5] and [6], which itself stem from [13].

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 [5] and [6], which itself stem from [13]. 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 [5] and [6] respectively. In these protection profiles it is an extension of the asset defined in [13]. This asset also includes ”SVD” (Integrity and Authenticity only), “SCD” of [14].

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 [5] and [6] respectively. In these protection profiles it is an extension of the asset defined in [13]. As for confidentiality, note that even though not each data element being transferred represents a secret, [16], [17] resp. require confidentiality of all transferred data by secure messaging in encrypt-then-authenticate mode. This asset also includes “DTBS” of [14].

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

7. Application note (taken from [20], application note 8)

The above secondary assets represent TSF and TSF-Data in the sense of CC.

3.1.2. Subjects

This ST 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 current 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 [7].

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 [7]. 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 [18].

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 document. This subject includes “Signatory” as defined [14].

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 [14].

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 [7], [18]) 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 [14].

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.

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

3.2.1. Threats from EAC1PP

This ST includes the following threats from [5]. 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 [5], cf. Chapter 3.2.3.

3.2.2. Threats from EAC2PP

This ST includes the following threats from the [6]. 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 [5] and [6] claim [13], and thus include the threats formulated in [13]. 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

The current ST also includes all threats of [14]. 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.

3.3. Organizational 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 [1], 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 [5], if the TOE contains EAC1-protected data.

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

Due to identical definitions and names, they are not repeated here. For the remaining OSPs from [5], see the next sections.

3.3.2. OSPs from EAC2PP

This ST includes the following OSPs from [6]. 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 [6], cf. the next section.

3.3.3. OSPs from PACEPP

This ST includes the following OSPs from [13], since both [5] and [6] claim [13]. 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.Trustworthy_PKI**

3.3.4. OSPs from SSCDPP

The current ST also includes all OSPs of [14]. 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. Additional OSPs

The next OSP addresses the need of a policy for the document manufacturer. It is formulated akin to [10].

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.

The ST includes the following OSP from [13], since both [5] and [6] claim [13], but the **P.Terminal** was extended because the Active Authentication protocol. The extension is marked with **bold** and the other part of the OSP remained unchanged.

P.Terminal

The PACE terminal shall operate their terminals as follows:

1. The related terminals (PACE terminal) shall be used by terminal operators and by travel document holders as defined in [9].
2. They shall implement the terminal parts of the PACE protocol [9], of the Passive Authentication [9] and use them in this order[3]. The PACE terminal shall use randomly and (almost) uniformly selected nonce, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann). **Furthermore the** PACE terminal **and** EAC1 terminal **shall implement the terminal parts of the Active Authentication protocol as described in [9].**
3. The related terminals need not to use any own credentials.
4. They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication(determination of the authenticity of data groups stored in the travel document, [9]).
5. The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the [13].

[3] This order is commensurate with [9].

Justification: The modification of **P.Terminal** is extended the original OSP in order to support the Active Authentication protocol. Taking into consideration the extension is not modify the original OSP, but added further requirements, this extension is not hurt the strict conformance as determined in PP Claim.

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 [5]. They concern EAC1-protected data.

- **A.Auth_PKI**
- **A.Insp_Sys**

Due to identical definitions and names, their definitions are not repeated here. For the remaining assumptions from [5], see the next sections.

3.4.2. Assumptions from EAC2PP

[6] only includes the assumption from [13] (see below) and defines no other assumption.

3.4.3. Assumptions from PACEPP

This ST includes the following assumptions from [13], since both [5] and [6] claim [13].

- **A.Passive_Auth**

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

3.4.4. Assumptions from SSCDPP

The current ST also includes all assumptions of [14]. These items are applicable, if the eSign application is included.

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

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

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.

OT.Chip_Auth_Proof_AA

Proof of the electronic documents authenticity with Active Authentication

The TOE must support the Terminal to verify the identity and authenticity of the electronic document as issued by the identified issuing State or Organisation by means of the Active Authentication protocol as defined in [7], [9]. The authenticity proof provided by electronic document shall be protected against attacks with high attack potential.

4.1.1. Security Objectives for the TOE from EAC1PP

This ST includes the following additional security objectives for the TOE from [5] that are not included in [13]. 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 [5], 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 [9]. The authenticity proof provided by electronic document's chip shall be protected against attacks with high attack potential.

Application note 8 (from ST author)

PACE-CAM enables much faster authentication of the of the chip than running PACE with General Mapping (according to [16]) 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 EAC2PP

This ST includes the following additional security objectives for the TOE from [6] that are not included in [13]. 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. For the remaining security objectives from [6], see the next sections.

4.1.3. Security Objectives for the TOE PACEPP

Both [5] and [6] claim [13]. 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 SSCDPP

The current ST also includes all security objectives for the TOE of [14]. 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_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 [13].

4.1.5. Additional Security Objectives 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 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 [10].

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 Objectives for the Operational Environment

4.2.1. Security Objectives from EAC1PP

This ST includes the following security objectives for the TOE from the [5]. 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

4.2.2. Security Objectives from EAC2PP

This ST includes the following security objectives for the TOE from the [6]. 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.

4.2.3. Security Objectives from PACEPP

Both [5] and [6] claim [13]. 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.

4.2.4. Security Objectives from SSCDPP

The current ST also includes all security objectives for the TOE of [14]. 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.

4.2.5. Additional Security Objectives for the Environment

The following objective on the environment is defined akin to the objective from [10].

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.

The following objectives on the environment are introduced because of the Active Authentication

- **OE.Auth_Key_AA**

Electronic document Active Authentication key pair

The issuing State or Organisation has to establish the necessary infrastructure in order to (i) generate the electronic document's Active Authentication Key Pair, (ii) sign (Passive Authentication) and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 and (iii) support Terminals of receiving States or Organisations to verify the authenticity of the electronic document used for genuine electronic document.

- **OE.Exam_Electronic_Document_AA**

Examination of the genuineness of the electronic document with Active Authentication

The Terminal of the receiving State or Organisation perform the Active Authentication protocol according to [7] and [9] in order to verify the genuineness of the presented electronic document.

4.3.Security Objective Rationale

Table 9 provides an overview of the security objectives' coverage. According to [1], 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 because of [20] or the newly introduced functions (i.e. **OE.Lim_Block_Loader**, **OT.Cap_Avail_Loader, OT.Chip_Auth_Proof_AA, OE.Auth_Key_AA, OE.Exam_Electronic_Document_AA and OT.Chip_Auth_Proof_PACE_CAM**) by checking the columns of Table 9 ,
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 or extended[4] threats, OSPs and assumptions by checking the rows of Table 9 , and
3. simply by checking the columns of Table 9 and the security objective rationales from the claimed PPs.

	OT.Chip_Auth_Proof_AA	OT.AC_Pers	OT.AC_Pers_EAC2	OT.Cap_Avail_Loader	OT.Chip_Auth_Proof_PACE_CAM	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Non_Interfere	OT.Sens_Data_Conf [5]	OT.Sens_Data_EAC2	OE.Auth_Key_AA	OE.Exam_Electronic_Document_AA	E.Lim_Block_Loader
T.InconsistentSec	-	X	X	X	-	X	X	X	X	X	X	-	-	X
T.Interfere	-	-	-	-	-	-	-	-	X	-	-	-	-	
T.Counterfeit	X	-	-	-	X	-	-	-	-	-	-	X	X	
P.Terminal	-	-	-	-	-	-	-	-	-	-	-	-	X	
P.Lim_Block_Loader	-	-	-	X	-	-	-	-	X	-	-	-	-	X

Table 9 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 [5]), 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.

[4] Only the impact of the modification is marked in the table.

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 [5]) is countered in [5] 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 of the chip than running PACE with general mapping followed by CA1.

Furthermore **T.Counterfeit** is countered by OT.Chip_Auth_Proof_AA, OE.Auth_Key_AA and OE.Exam_Electronic_Document_AA. These security objectives addresses the implementation of the Active Authentication and thus counters the thread of counterfeiting an electronic document containing an ePassport application. It ensures that the chip supports the Active Authentication protocol, which supports to verify that the electronic document is genuine (similar as Chip Authentication without secure messaging).

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.

The OSP **P.Terminal** is extended to support the Active Authentication protocol. With this extension the **P.Terminal** countered by the security objective **OE.Exam_Electronic_Document_AA**. The **OE.Exam_Electronic_Document_AA** enforces the terminal parts of the Active Authentication.

5. EXTENDED COMPONTENTS DEFINITION

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

- FAU_SAS.1 from the family FAU_SAS from [13]
- FCS_RND.1 from the family FCS_RND from [13]
- FMT_LIM.1 and FMT_LIM.2 from the family FMT_LIM [13]
- FPT_EMS.1 from the family FPT_EMS from [13]
- FIA_API.1 from the family FIA_API from [6]

For precise definitions we refer to [13] and [6].

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 [1]. 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 to be filled in by the ST author appear in square brackets with an indication that a selection has to be made, [selection:], and are *italicized*. 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 to be filled in by the ST author appear in square brackets with an indication that an assignment has to be made [assignment:], and are *italicized*. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicized *like this*. 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 [5],

/EAC2PP or /XXX_EAC2PP for [6],

and /SSCDPP or /XXX_SSCDPP for [14].

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.

Despite this ST claims strict conformance to [13], SFRs can be safely ignored in this ST as long as [5] and [6] 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). Three cases are distinguished:

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 [5] and [6]. 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 [5] and [6].
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 [5] and [6]. Such a case is also explicitly mentioned in the text.

Thus internal consistency is not violated.

6.1.1. Class FCS

The following SFRs are imported due to claiming [6]. They concern cryptographic support for applications that contain EAC2-protected data groups.

- **FCS_CKM.1/DH_PACE_EAC2PP**
- **FCS_COP.1/SHA_EAC2PP**
- **FCS_COP.1/SIG_VER_EAC2PP**
- **FCS_COP.1/PACE_ENC_EAC2PP**
- **FCS_COP.1/PACE_MAC_EAC2PP**
- **FCS_CKM.4/EAC2PP**
- **FCS_RND.1/EAC2PP**

FCS_CKM.1/DH_PACE_EAC2PP
Cryptographic Key Generation – Diffie-Hellman for PACE and CA2 Session Keys

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 Diffie-Hellman-Protocol compliant to [27] and ECDH compliant to [26]][5][6] and specified cryptographic key sizes AES 128, 192, 256[7] that meet the following: **[17]**[8]

9. Application note (taken from [6], application note 10)

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

[6] [selection: *Diffie-Hellman-Protocol compliant to [27] , ECDH compliant to [26]*]

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

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

In the above and all subsequent related SFRs, the reference w.r.t. the PACE protocol is changed to [17], whereas [13] references [7]. The difference between the two definitions is that [17] defines additional optional parameters for the command MSE:Set AT. This optional parameters (e.g. the CHAT) are technically required, since here Terminal Authentication 2 (TA2) can be executed right after PACE (see FIA_UID.1/EAC2_Terminal_EAC2PP). As [7] does not consider TA2, no such definition is given there. These additional parameters are optional and not used during PACE itself (only afterwards). If PACE is run without TA2 afterwards, access to data on the chip is given as specified by [13]. If TA2 is run afterwards, access to data on the chip can be further restricted w.r.t. to the authorization level of the terminal. Therefore, this change of references does not violate strict conformance to [13]. We treat this change of references as a refinement operation, and thus mark the changed reference using **bold** text.

10. Application note (redefined by ST author, taken from [6], application note 11)

Applied.

11. Application note (taken from [6], application note 12)

[13] considers Diffie-Hellman key generation only for PACE. Since the TOE is required to implement Chip Authentication 2 (cf. FIA_API.1/CA_EAC2PP), here FCS_CKM.1/DH_PACE_EAC2PP applies for CA2 as well.

FCS_COP.1/SHA_EAC2PP
Cryptographic operation – Hash for key derivation

Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] 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.
	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[9] in accordance with a specified cryptographic algorithm SHA-1, SHA-224, SHA-256, SHA-384, SHA-512[10] and cryptographic key sizes none[11] that meet the following: [28][12].

12. Application note (taken from [6], application note 13)

For compressing (hashing) an ephemeral public key for DH (TA2 and CA2), the hash function SHA-1 shall be used ([18]). The TOE shall implement as hash functions either SHA-1 or SHA-224 or SHA-256 for Terminal Authentication 2, cf. [18]. Within the normative Appendix of [18] '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
Cryptographic operation – Signature verification

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[13]. 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/EAC2PP below), the current ST does not contain any dedicated requirement like FDP_ITC.2 for the import function.
	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.

[9] [assignment: *list of cryptographic operations*]
[10] [assignment: *cryptographic algorithm*]
[11] [assignment: *cryptographic key sizes*]
[12] [assignment: *list of standards*]
[13] as already mentioned, operational use of the TOE is explicitly in focus of the ST and in the [20]

FCS_COP.1.1/SIG_VER_EAC2PP

The TSF shall perform digital signature verification[14] in accordance with a specified cryptographic algorithm RSA, RSA CRT and ECDSA[15] and cryptographic key sizes RSA: RSA, RSA CRT: 1024, 1280, 1536, 1984, 2048, 3072, 4096 and from 2000 bit to 4096 bit in one bit steps; ECDSA: 160, 192, 224, 256, 320, 384, 521 bit[16] that meet the following: [24], [29][17].

13. Application note (taken from [6], application note 14)

This SFR is concerned with Terminal Authentication 2, cf. [17].

14. Application note (from ST author)

The TOE based on the Platform functionalities supports RSA and RSA-CRT digital signature algorithms and cryptographic key sizes 512 bits up to 4096 bits with equal security measures. However, to fend off attackers with high attack potential an adequate key length must be used.

FCS_COP.1/PACE_ENC_EAC2PP
Cryptographic operation – Encryption/Decryption AES

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

[14] [assignment: *list of cryptographic operations*]

[15] [assignment: *cryptographic algorithm*]

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

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

The TSF shall perform secure messaging – encryption and decryption[18] in accordance with a specified cryptographic algorithm AES in CBC mode[19] and cryptographic key sizes 128, 192, 256 bit[20] that meet the following: **[18]**[21]

15. Application note (taken from [6], application note 15)

This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol (PACE-K_{Enc}) or Chip Authentication 2 (CA-K_{Enc}) according to FCS_CKM.1/DH_PACE_EAC2PP. Note that in accordance with [18], 3DES could be used in CBC mode for secure messaging. Due to the fact that 3DES is not recommended any more (cf. [17]), 3DES in any mode is no longer applicable here.

16. Application note (taken from [6], application note 16)

Refinement of FCS_COP.1.1/PACE_ENC_EAC2PP, since here PACE must adhere to [18]. All references (both the one in [13] and [18]) itself reference [12] for secure messaging. [18] however further restricts the available choice of key-sizes and algorithms. Hence, [18] is fully (backward) compatible to the reference given in [13].

FCS_COP.1/PACE_MAC_EAC2PP
Cryptographic operation – MAC

Hierarchical to:	No other components
Dependencies:	FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/DH_PACE_EAC2PP
	FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/EAC2PP

FCS_COP.1.1/PACE_MAC_EAC2PP

[18] [assignment: *list of cryptographic operations*]
[19] [selection: *cryptographic algorithm*]
[20] [selection: *128, 192, 256 bit*]
[21] [assignment: *list of standards*]

The TSF shall perform secure messaging – message authentication code[22] in accordance with a specified cryptographic algorithm CMAC[23] and cryptographic key sizes 128, 192, 256 bit[24] that meet the following: **[18]**[25]

17. Application note (redefined by ST author, taken from [6], application note 17)

See 16. Application note (taken from [6], application note 16).

18. Application note (taken from [6], application note 18)

This SFR removes 3DES and restricts to CMAC compared to the SFR of [13] by selection. Hence, a minimum key-size of 128 bit is required.

FCS_CKM.4/EAC2PP
Cryptographic key destruction – Session keys

Hierarchical to:	No other components
Dependencies:	FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/DH_PACE_EAC2PP and FCS_CKM.1/CA_EAC1PP

FCS_CKM.4.1/EAC2PP

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physically overwriting the keys in a randomized manner[26] that meets the following: provided by the underlying certified Platform[27].

19. Application note

In [13] 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/EAC2PP 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/EAC2PP.

[22] [assignment: *list of cryptographic operations*]

[23] [selection: *cryptographic algorithm*]

[24] [selection: *112 128, 192, 256 bit*]

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

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

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

FCS_RND.1/EAC2PP
Quality metric for random numbers

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 DRG.3[28].

20. Application note

In [13] concerning this component requires the TOE to generate random numbers (random nonce) for PACE. While the definition of FCS_RND.1/EAC2PP 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/PACE_EAC2PP.

The following SFRs are imported due to claiming [5]. They concern cryptographic support for applications that contain EAC1-protected data groups.

- **FCS_CKM.1/DH_PACE_EAC1PP**
- **FCS_CKM.4/EAC1PP**

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

- **FCS_COP.1/PACE_ENC_EAC1PP**
- **FCS_COP.1/PACE_MAC_EAC1PP**

21. Application note (redefined by ST author, taken from[20], application note 9)

Applied.

- **FCS_RND.1/EAC1PP**

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

- **FCS_CKM.1/CA_EAC1PP**
- **FCS_COP.1/CA_ENC_EAC1PP**
- **FCS_COP.1/SIG_VER_EAC1PP**
- **FCS_COP.1/CA_MAC_EAC1PP**

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

FCS_CKM.1/DH_PACE_EAC1PP
Cryptographic key generation – Diffie-Hellman for PACE session keys

Hierarchical to: No other components

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

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

FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4/EAC1PP

FCS_CKM.1.1/DH_PACE_EAC1PP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Diffie-Hellman-Protocol compliant to [27], ECDH compliant to [26][29][30] and specified cryptographic key sizes TDES 128, AES 128, 192 and 256 bits[31] that meet the following:[7][32]

FCS_COP.1/PACE_ENC_EAC1PP
Encryption / Decryption AES / 3DES

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE_EAC1PP.

FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4/EAC1PP.

FCS_COP.1.1/PACE_ENC_EAC1PP

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

[30] [selection: *Diffie-Hellman-Protocol compliant to [27] , ECDH compliant to [26]*]

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

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

The TSF shall perform secure messaging – encryption and decryption[33] in accordance with a specified cryptographic algorithm *AES, 3DES*[34] in CBC mode[35] and cryptographic key sizes 3DES 112, AES 128, 192, 256 bit[36][37] that meet the following: compliant to [7][38].

FCS_COP.1/PACE_MAC_EAC1PP
Cryptographic operation – MAC

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE_EAC1PP

FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4/EAC1PP.

FCS_COP.1.1/PACE_MAC_EAC1PP

The TSF shall perform secure messaging – message authentication code[39] in accordance with a specified cryptographic algorithm CMAC, Retail-MAC[40][41] and cryptographic key sizes 3DES 112, AES 128, 192, 256 bit[42][43] that meet the following: compliant to [7][44].

FCS_CKM.1/CA_EAC1PP
Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys

Hierarchical to: No other components

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

[33] [assignment: *list of cryptographic operations*]
[34] [selection: *AES, 3DES*]
[35] [assignment: *cryptographic algorithm*]
[36] [assignment: *cryptographic key sizes*]
[37] [selection: *112, 128, 192, 256*]
[38] [assignment: *list of standards*]
[39] [assignment: *list of cryptographic operations*]
[40] [assignment: *cryptographic algorithm*]
[41] [selection: *CMAC, Retail-MAC*]
[42] [assignment: *cryptographic key sizes*]
[43] [selection: *112, 128, 192, 256*]
[44] [assignment: *list of standards*]

FCS_COP.1/CA_ENC_EAC1PP and
FCS_COP.1/CA_MAC_EAC1PP

FCS_CKM.4 Cryptographic key destruction fulfilled by
FCS_CKM.4/EAC1PP.

FCS_CKM.1.1/CA_EAC1PP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Diffie-Hellman protocol compliant to PKCS#3 and based on an ECDH protocol[45] and specified cryptographic key sizes TDES 112, AES 128, 192 and 256 bits[46] that meet the following:based on the Diffie-Hellman key derivation protocol compliant to [27] and [16] , based on an ECDH protocol compliant to [26][47][48]

22. Application note (taken from [5], application note 12)

FCS_CKM.1/CA_EAC1PP implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [16].

23. Application note (taken from [5], application note 13)

The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [16]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [27]) or on the ECDH compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm) (cf. [26], for details). The shared secret value is used to derive the Chip Authentication Session Keys used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [16]).

24. Application note (taken from [5], application note 14)

The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms. The Chip Authentication Protocol v.1 may use SHA-1 (cf. [16]). The TOE may implement additional hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol v.1 (cf. [16] for details).

25. Application note (taken from [5], application note 15)

The TOE shall destroy any session keys in accordance with FCS_CKM.4 from [13] after (i) detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication Protocol v.1. (iii) The TOE shall destroy the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys. (iv) The TOE shall clear the memory area of any

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

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

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

[48] [selection: *based on the Diffie-Hellman key derivation protocol compliant to [27] and [16] , based on an ECDH protocol compliant to [26]*]

session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1/EAC1PP. Concerning the Chip Authentication keys FCS_CKM.4/EAC1PP is also fulfilled by FCS_CKM.1/CA_EAC1PP.

FCS_COP.1/CA_ENC_EAC1PP
Cryptographic operation – Symmetric Encryption / Decryption

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/EAC1PP

FCS_COP.1.1/CA_ENC_EAC1PP

The TSF shall perform secure messaging – encryption and decryption[49] in accordance with a specified cryptographic algorithm Triple-DES and AES[50] and cryptographic key sizes Triple-DES:112, AES: 128, 192 and 256 bits[51] that meet the following:[16][52].

26. Application note (taken from [5], application note 16)

This SFR requires the TOE to implement the cryptographic primitives (e.g. Triple-DES and/or AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA_EAC1PP.

FCS_COP.1/SIG_VER_EAC1PP
Cryptographic operation – Signature verification by electronic document

Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/CA_EAC1PP

[49] [assignment: *list of cryptographic operations*]
[50] [assignment: *cryptographic algorithm*]
[51] [assignment: *cryptographic key sizes*]
[52] [assignment: *list of standards*]

	FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/EAC1PP

FCS_COP.1.1/SIG_VER_EAC1PP

The TSF shall perform digital signature verification[53] in accordance with a specified cryptographic algorithm RSA v1.5 with SHA-256 and SHA-512, RSA-PSS with SHA-256 and SHA-512, ECDSA with SHA-256, SHA-224, SHA-384 and SHA-512[54] and cryptographic key sizes RSA 2048, 4096 and from 2000 bit to 4096 bit in one bit steps, ECDSA 160, 192, 224, 256, 320, 384, 521 bits[55] that meet the following: [24][29][56].

27. Application note (redefined by ST author, taken from [5], application note 17)

Applied.

28. Application note (from ST author)

The TOE based on the Platform functionalities supports RSA and RSA-CRT digital signature algorithms and cryptographic key sizes 512 bits up to 4096 bits with equal security measures. However, to fend off attackers with high attack potential an adequate key length must be used.

FCS_COP.1/CA_MAC_EAC1PP
Cryptographic operation – MAC

Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/CA_EAC1PP
	FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/EAC1PP

FCS_COP.1.1/CA_MAC_EAC1PP

[53] [assignment: *list of cryptographic operations*]
[54] [assignment: *cryptographic algorithm*]
[55] [assignment: *cryptographic key sizes*]
[56] [assignment: *list of standards*]

The TSF shall perform secure messaging – message authentication code[57] in accordance with a specified cryptographic algorithm CMAC or Retail-MAC[58] and cryptographic key sizes 112, 128, 192 and 256 bits[59] that meet the following: [16][60].

29. Application note (taken from [5], application note 18)

This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA_EAC1PP. Furthermore, the SFR is used for authentication attempts of a terminal as Personalisation Agent by means of the authentication mechanism.

The following SFRs are defined because the TOE supports the Chip Authentication version 2 and Restricted Identification key pair(s) generation on the TOE as described in FMT_MTD.1/SK_PICC_EAC2PP.

FCS_CKM.1/CA2
Cryptographic key generation – Chip Authentication version 2 Key pair(s)

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/CA2

The TSF shall generate cryptographic keys **to Chip Authentication 2** in accordance with a specified cryptographic key generation algorithm RSA or ECC[61] and specified cryptographic key sizes 1024, 1280, 1536, 1984, 2048, 3072 and 4096 bits or 160, 192, 224, 256, 384 and 521 bits [62] that meet the following: [31][63].

30. Application note (from ST author)

The TOE supports to create Chip Authentication version 2 Key pair(s) on the TOE as described in FMT_MTD.1/SK_PICC_EAC2PP. The TOE generates the key pair(s) in secure way, but the

[57] [assignment: *list of cryptographic operations*]
[58] [assignment: *cryptographic algorithm*]
[59] [assignment: *cryptographic key sizes*]
[60] [assignment: *list of standards*]
[61] [assignment: *cryptographic key generation algorithm*]
[62] [assignment: *cryptographic key sizes*]
[63] [assignment: *list of standards*]

appropriate key size shall be assessed during the personalization of the TOE. The refinement was necessary for the sake of clarity.

FCS_CKM.1/RI
Cryptographic key generation – Restricted Identification Key pair (s)

Hierarchical to:	No other components
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] not fullfilled but justified: the crypgographic part of Restricted Identification protocol is not part of the TOE, so no cryptographic operation is related to FCS_CKM.1/RI. FCS_CKM.4 Cryptographic key destruction fullfilled by FCS_CKM.4/EAC2PP

FCS_CKM.1.1/RI

The TSF shall generate cryptographic keys **to Restricted Identification** in accordance with a specified cryptographic key generation algorithm RSA or ECC[64] and specified cryptographic key sizes 1024, 1280, 1536, 1984, 2048, 3072 and 4096 bits or 160, 192, 224, 256, 384 and 521 bits[65] that meet the following: [31][17][66].

31. Application note (from ST author)

The TOE supports to create Restricted Identification Key pair(s) on the TOE as described in FMT_MTD.1/SK_PICC_EAC2PP. The TOE generates the key pair(s) in secure way, but the appropriate key size shall be assessed during the personalization of the TOE. The refinement was necessary for the sake of clarity.

The following SFRs are new and concern cryptographic support for ePassport application in combination with [5] in case the Active Authentication protocol is active:

- **FCS_CKM.1/AA**
- **FCS_COP.1/AA**

FCS_CKM.1/AA
Cryptographic key generation – Active Authentication Key Pair

Hierarchical to:	No other components

[64] [assignment: *cryptographic key generation algorithm*]
[65] [assignment: *cryptographic key sizes*]
[66] [assignment: *list of standards*]

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

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/EAC1PP

FCS_CKM.1.1/AA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA or ECDSA[67] and specified cryptographic key sizes 1024, 1280, 1536, 1984, 2048, 3072 and 4096 bits or 160, 192, 224, 256, 384 and 521 bits[68] that meet the following: [7][9][69].

FCS_COP.1/AA
Cryptographic operation – Active Authentication

Hierarchical to: No other components

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

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/EAC1PP

FCS_COP.1.1/AA

The TSF shall perform digital signature creation[70] in accordance with a specified cryptographic algorithm RSA or ECDSA[71] and . cryptographic key sizes RSA with key sizes 2048-4096 and ECDSA with key sizes 160-521[72] that meet the following: [7][9][73].

The following SFRs are new and concerns cryptographic support for ePassport applications in combination with [5].

- **FCS_CKM.1/CAM**

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

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

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

[70] [assignment: *list of cryptographic operations*]

[71] [assignment: *cryptographic algorithm*]

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

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

- **FCS_COP.1/CAM**

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/CAM FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/EAC1PP

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[74] and specified cryptographic key sizes AES 128, 192 and 256 bit[75] that meet the following: [9][76].

32. Application note (from ST author)

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.[9].

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

[74] [assignment: *cryptographic key generation algorithm*]
[75] [assignment: *cryptographic key sizes*]
[76] [assignment: *list of standards*]

	FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/EAC1PP

FCS_COP.1.1/CAM

The TSF shall perform the PACE-CAM protocol[77] in accordance with a specified cryptographic algorithm PACE-CAM[78] and cryptographic key sizes AES 128, 192 and 256 bits[79] that meet the following:[9][80]

33. Application note (from ST author)

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 [14]. They only concern the cryptographic support for an eSign application.

- **FCS_CKM.1/SSCDPP**
- **FCS_CKM.4/SSCDPP**

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

- **FCS_COP.1/SSCDPP**

FCS_CKM.1/SSCDPP
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/SSCDPP
	FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/EAC2PP

FCS_CKM.1.1/SSCDPP

[77] [assignment: *list of cryptographic operations*]
[78] [assignment: *cryptographic algorithm*]
[79] [assignment: *cryptographic key sizes*]
[80] [assignment: *list of standards*]

The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm RSA or ECDSA[81] and specified cryptographic key sizes 1024, 1280, 1536, 1984, 2048, 3072 and 4096 bits or 160, 192, 224, 256, 384 and 521 bits[82] that meet the following: [23][83].

34. Application note (taken from [14], application note 5)

The ST writer performed the missing operations in the element FCS_CKM.1.1/SSCDPP. The refinement in the element FCS_CKM.1.1 SSCDPP substitutes "cryptographic keys" by "SCD/SVD pairs" because it clearly addresses the SCD/SVD key generation.

FCS_COP.1/SSCDPP
Cryptographic operation

Hierarchical to:	No other components
Dependencies:	FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attribute or FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/SSCDPP FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/EAC2PP

FCS_COP.1.1/SSCDPP

The TSF shall perform digital signature creation[84] in accordance with a specified cryptographic algorithm RSA according to RSASSA-PKCS1-v1_5, RSASSA-PSS or ECDSA according to ISO14883-3[85] and . cryptographic key sizes RSA with key sizes 2048-4096 and ECDSA with key sizes 160-521[86] that meet the following: [24] [29][87].

35. Application note (taken from [14], application note 7)

Applied.

36. Application note (from ST author)

The underlying Platform supports RSA, RSA-CRT and ECDSA digital signature algorithms and cryptographic key sizes 2048 bits to 4096 bits (RSA) and 160 bits to 521 bits (ECDSA) with

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

equal security measures. However, to fend off attackers with high attack potential an adequate key length must be used

6.1.2. Class FIA

Table 10 provides an overview of the authentication and identification mechanisms used.

Name	SFR for the TOE
PACE protocol	FIA_UID.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
Active Authentication	FIA_API.1/AA FIA_UAU.1/PACE_EAC1PP FIA_UAU.4/PACE_EAC1PP
Restricted Identification	FIA_API.1/RI_EAC2PP
eSign-PIN	FIA_UAU.1/SSCDPP

Table 10 Overview of authentication and identification SFRs

6.1.2.1. SFRs for EAC2-protected Data

The following SFRs are imported due to claiming [6]. They mainly concern authentication mechanisms related to applications with EAC2-protected data.

- **FIA_AFL.1/Suspend_PIN_EAC2PP**
- **FIA_AFL.1/Block_PIN_EAC2PP**
- **FIA_API.1/CA_EAC2PP**
- **FIA_API.1/RI_EAC2PP**
- **FIA_UID.1/PACE_EAC2PP**
- **FIA_UID.1/EAC2_Terminal_EAC2PP**

37. Application note (taken from [20], application note 10)

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.

- **FIA_UAU.1/PACE_EAC2PP**
- **FIA_UAU.1/EAC2_Terminal_EAC2PP**
- **FIA_UAU.4/PACE_EAC2PP**

38. Application note (taken from [6], application note 26)

For PACE, the TOE randomly selects an almost uniformly distributed nonce of 128 bit length. The [20] and the current ST support a key derivation function based on AES; see [17]. For TA2, the TOE randomly selects a nonce r_{PICC} of 64 bit length, see [17]. This SFR extends FIA_UAU.4/PACE_EAC1PP from [13] by assigning the authentication mechanism Terminal Authentication 2.

- **FIA_UAU.5/PACE_EAC2PP**
- **FIA_UAU.6/CA_EAC2PP**
- **FIA_AFL.1/PACE_EAC2PP**
- **FIA_UAU.6/PACE_EAC2PP**

FIA_AFL.1/Suspend_PIN_EAC2PP
Authentication failure handling – Suspending PIN

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 an administrator configurable positive integer within [1-127][88] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using the PIN as the shared password for PACE[89].

FIA_AFL.1.2/Suspend_PIN_EAC2PP

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

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

When the defined number of unsuccessful authentication attempts has been met[90], the TSF shall suspend the reference value of the PIN according to [17][91].

39. Application note (taken from [6], application note 19)

This SFR is not in conflict to FIA_AFL.1 from [13], 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
Authentication failure handling – Blocking PIN

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 when an administrator configurable positive integer within [1-127][92] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using the suspended[93] PIN as the shared password for PACE[94].

FIA_AFL.1.2/Block_PIN_EAC2PP

When the defined number of unsuccessful authentication attempts has been met[95], the TSF shall block the reference value of PIN according to [17][96].

FIA_API.1/CA_EAC2PP
Authentication Proof of Identity

Hierarchical to: No other components

Dependencies: No dependencies

FIA_API.1.1/CA_EAC2PP

[90] [selection: *met , surpassed*]
[91] [assignment: *list of actions*]
[92] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]*
[93] as required by FIA_AFL.1/Suspend_PIN_EAC2PP
[94] [assignment: *list of authentication events*]
[95] [selection: *met , surpassed*]
[96] [assignment: *list of actions*]

The TSF shall provide the protocol Chip Authentication 2 according to [17][97], to prove the identity of the TOE[98].

FIA_API.1/RI_EAC2PP
Authentication Proof of Identity

Hierarchical to: No other components

Dependencies: No dependencies

FIA_API.1.1/RI_EAC2PP

The TSF shall provide the Restricted Identification protocol according to [17][99], to prove the identity of the TOE[100].

40. Application note (taken from [6], application note 20)

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 [17], and thus the above SFR only applies if Restricted Identification is supported by the TOE.

FIA_UID.1/PACE_EAC2PP
Timing of identification

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 [17]
3. to read the Initialization Data if it is not disabled by TSF according to ~~**FMT_MTD.1/INI_DIS**~~**FMT_MTD.1/INI_DIS_EAC2PP**[101]

[97] [assignment: *authentication mechanism*]
[98] [assignment: *authorised user or role, or of the TOE itself*]
[99] [assignment: *authentication mechanism*]
[100] [assignment: *authorized user or role*]
[101] [assignment: *list of TSF-mediated actions*]

4. none[102]

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.

41. Application note (taken from [6], application note 21)

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 Holder itself, an authorized person other than the Electronic Document Holder, or a device.

42. Application note (from ST author)

The refinement was necessary to ensure unified terminology usage of SFRs.

FIA_UID.1/EAC2_Terminal_EAC2PP Timing of identification

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 [17],
3. to read the Initialization Data if it is not disabled by TSF according to ~~**FMT_MTD.1/INI_DIS**~~**FMT_MTD.1/INI_DIS_EAC2PP**
4. carrying out the Terminal Authentication protocol 2 according to [17][103]
5. none[104]

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

FIA_UID.1.2/EAC2_Terminal_EAC2PP

[102] [assignment: *list of TSF-mediated actions*]
[103] [assignment: *list of TSF-mediated actions*]
[104] [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.

43. Application note (taken from [6], application note 22)

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

44. Application note (taken from [6], application note 23)

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. [17]).

45. Application note (from ST author)

The refinement was necessary to ensure unified terminology usage of SFRs.

FIA_UAU.1/PACE_EAC2PP
Timing of authentication

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 [17],
3. to read the Initialization Data if it is not disabled by TSF according to ~~FMT_MTD.1/INI_DIS~~**FMT_MTD.1/INI_DIS_EAC2PP**,
4. none[105]

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

FIA_UAU.1.2/PACE_EAC2PP

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

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

46. Application note (taken from [6], application note 24)

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_EAC2PP. 44. Application note (taken from [6], application note 23) also applies here.

47. Application note (from ST author)

The refinement was necessary to ensure unified terminology usage of SFRs.

FIA_UAU.1/EAC2_Terminal_EAC2PP Timing of authentication

Hierarchical to:	No other components
Dependencies:	[FIA_UID.1 Timing of identification]: fulfilled by FIA_UAU.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 [17],
3. to read the Initialization Data if it is not disabled by TSF according to ~~FMT_MTD.1/INI_DIS~~**FMT_MTD.1/INI_DIS_EAC2PP**
4. carrying out the Terminal Authentication protocol 2 according to [17][106]

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.

48. Application note (taken from [6], application note 25)

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_EAC2PP 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.

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

49. Application note (from ST author)

The refinement was necessary to ensure unified terminology usage of SFRs.

FIA_UAU.4/PACE_EAC2PP
Single-use authentication of the Terminals by the TOE

Hierarchical to:	No other components
Dependencies:	No dependencies

FIA_UAU.4.1/PACE_EAC2PP

The TSF shall prevent reuse of authentication data related to:

1. PACE protocol according to [17],
2. Authentication Mechanism based on AES[107]
3. Terminal Authentication 2 protocol according to [17].[108]
4. none[109]

50. Application note (taken from [6], application note 26)

For PACE, the TOE randomly selects an almost uniformly distributed nonce of 128 bit length. The [6] supports a key derivation function based on AES; see [17]. For TA2, the TOE randomly selects a nonce r_{PICC} of 64 bit length, see [17]. This SFR extends FIA_UAU.4/PACE from [13] by assigning the authentication mechanism Terminal Authentication 2.

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 **[17]**,
2. Passive Authentication according to [8]
3. Secure messaging ~~**in MAC-ENC**~~ mode according to **[18]**
4. Symmetric Authentication Mechanism based on TDES and AES[110][111]

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

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

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

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

[111] [selection: *AES or other approved algorithms*]

5. Terminal Authentication 2 protocol according to [17],
6. Chip Authentication 2 according to [17][112][113]
7. none[114]

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 (Device authentication) according to [30][115]
3. The TOE accepts the authentication attempt by means of the Terminal Authentication 2 protocol,only if (i) the terminal presents its static public key PK_{PCD} and the key is successfully verifiable up to the CVCA and (ii) the terminal uses the PICC identifier IDP_{ICC} = Comp(ephem-PK_{PICC}-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.[116]
5. none[117]

51. Application note (taken from [6], application note 27)

Refinement of FIA_UAU.5.2/PACE_EAC2PP, since here PACE must adhere to [17] and [18], cf. 9. Application note (taken from [6], application note 10). Since the formulation "MAC-ENC mode" is slightly ambiguous (there is only one secure messaging mode relevant both in [13] and here, and it is actually the same in both references), it is removed here by refinement in the third bullet point of FIA_UAU.5.1/PACE_EAC2PP.

Remark: Note that 5. and 6. in FIA_UAU.5.1/PACE_EAC2PP and 3. and 4. of FIA_UAU.5.2/PACE_EAC2PP are additional assignments (using the open assignment operation) compared to [13].

52. Application note (from ST author)

[112] Passive Authentication using SO_C is considered to be part of CA2 within this ST.
[113] [assignment: *list of multiple authentication mechanisms*]
[114] [assignment: *list of multiple authentication mechanisms*]
[115] [selection: *the Authentication Mechanism with Personalization Agent Key(s)*]
[116] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
[117] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

Symmetric Authentication Mechanism implemented according to [30].

FIA_UAU.6/CA_EAC2PP
Re-authenticating of Terminal by the TOE

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[118].

FIA_AFL.1/PACE_EAC2PP
Authentication failure handling – PACE authentication using non-blocking authorisation data

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 an administrator configurable positive integer number within [1-127][119] unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password.[120]

FIA_AFL.1.2/PACE_EAC2PP

When the defined number of unsuccessful authentication attempts has been met[121], the TSF shall delay each following authentication attempt until the next successful authentication.[122].

53. Application note (from ST author)

In line with [6] the shared password for PACE can be CAN, MRZ, PIN and PUK. The specific case of PIN is detailed in FIA_AFL.1/Suspend_PIN_EAC2PP and

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

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

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

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

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

FIA_AFL.1/Block_PIN_EAC2PP and furthermore 39. Application note (taken from [6], application note 19).

FIA_UAU.6/PACE_EAC2PP
Re-authenticating of Terminal by the TOE

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.[123]

6.1.2.2. SFRs for EAC1-protected data

- **FIA_UID.1/PACE_EAC1PP**
- **FIA_UAU.1/PACE_EAC1PP**
- **FIA_UAU.4/PACE_EAC1PP**
- **FIA_UAU.5/PACE_EAC1PP**
- **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**
- **FIA_API.1/EAC1PP**
- **FIA_AFL.1/PACE_EAC1PP**

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

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:

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

1. to establish the communication channel,
2. carrying out the PACE Protocol according to [7],
3. to read the Initialization Data if it is not disabled by TSF according to ~~FMT_MTD.1/INI_DIS~~ FMT_MTD.1/INI_DIS_EAC1PP
4. to carry out the Chip Authentication Protocol v.1 according to [16] **or the Chip Authentication mapping (PACE-CAM) according to [9].**
5. to carry out the Terminal Authentication Protocol v.1 according to [16] **resp. according to [9] if PACE-CAM is used.**[124]
6. none[125].

on behalf of the user to be performed before the user isidentified.

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.

54. Application note (from ST author)

The SFR is refined here in order for the TSF to *additionally* provide the PACE-CAM protocol by referencing [9]. PACE-CAM combines PACE and Chip Authentication 1 for faster execution times. Hence, a TOE meeting the original requirement also meets the refined requirement.

55. Application note (taken from [5], application note 20)

The SFR FIA_UID.1/PACE in [5] covers the definition in [13] and extends it by EAC aspect 4. This extension does not conflict with the strict conformance to [13].

56. Application note (taken from [5], application note 21)

In the Phase 2 “Manufacturing” the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalisation Data in the audit records of the IC. The electronic document manufacturer may create the user role Personalisation Agent for transition from Phase 2 to Phase 3 “Personalisation of the Electronic Document”. The users in role Personalisation Agent identify themselves by means of selecting the authentication key. After personalisation in the Phase 3 the PACE domain parameters, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may identify itself as (i) EAC1 terminal by selection of the templates for the Terminal Authentication Protocol Version 1 or (ii) if necessary and available by authentication as Personalisation Agent (using the Personalisation Agent Key).

57. Application note (taken from [5], application note 22)

[124] [assignment: *list of TSF-mediated actions*]
[125] [assignment: *list of TSF-mediated actions*]

User identified 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 electronic document holder itself or an authorised other person or device (PACE terminal).

58. Application note (taken from [5], application note 23)

In the life-cycle phase 'Manufacturing' the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialisation Data and/or Pre-personalisation Data in the audit records of the IC.

Please note that a Personalisation Agent acts on behalf of the electronic document Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalisation Agents. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role 'Personalisation Agent', when a terminal proves the respective Terminal Authorisation Level as defined by the related policy (policies).

59. Application note (from ST author)

The refinement was necessary to ensure unified terminology usage of SFRs.

FIA_UAU.1/PACE_EAC1PP
Timing of authentication

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 [7],
3. to read the Initialization Data if it is not disabled by TSF according to ~~FMT_MTD.1/INI_DIS~~ **FMT_MTD.1/INI_DIS_EAC1PP** ,
4. to identify themselves by selection of the authentication key
5. to carry out the Chip Authentication Protocol Version 1 according to [16]
6. to carry out the Terminal Authentication Protocol Version 1 according to [16][126]
7. to carry out the Active Authetnication Mechanism according to [9][127]

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

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

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.

60. Application note (taken from [5], application note 24)

The SFR FIA_UAU.1/PACE_EAC1PP in the current ST covers the definition in [13] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to [13].

61. Application note (taken from [5], application note 25)

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 electronic document holder itself or an authorised another person or device (PACE terminal).

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.

62. Application note (from ST author)

The refinement was necessary to ensure unified terminology usage of SFRs.

FIA_UAU.4/PACE_EAC1PP
Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.4.1/PACE_EAC1PP

The TSF shall prevent reuse of authentication data related to

1. PACE Protocol according to [7],
2. Authentication Mechanism based on Triple-DES or AES[128]
3. Terminal Authentication Protocol v.1 according to [16].[129]
4. **Active Authentication protocol according to [7], [9]**

63. Application note (taken from [5], application note 26)

The SFR FIA_UAU.4.1/PACE_EAC1PP in the current ST covers the definition in [13] and extends it by the EAC aspect 3. This extension does not conflict with the strict conformance to [13]. The generation of random numbers (random nonce) used for the authentication protocol

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

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

(PACE) and Terminal Authentication as required by FIA_UAU.4/PACE_EAC1PP is required by FCS_RND.1 from [13].

64. Application note (taken from [5], application note 27)

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.

65. Application note (ST author)

The refinement was necessary because the authentication data (nonce) is must not be reused during Active Authentication protocol according to [9].

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 according to [7] **and PACE-CAM protocol according to [9]**
2. Passive Authentication according to [8]
3. Secure messaging in MAC-ENC mode according to [7].
4. Symmetric Authentication Mechanism based on Triple-DES or AES[130]
5. Terminal Authentication Protocol v.1 according to [16],[131]

to support user authentication

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.

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

[131] [assignment: *list of multiple authentication mechanism*]

2. The TOE accepts the authentication attempt as Personalisation Agent by the Symmetric Authentication (Device authentication) according to [30][132]
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.**[133]
5. none[134]

66. Application note (from ST author)

The SFR is refined here in order for the TSF to additionally provide the PACE-CAM protocol by referencing [9]. PACE-CAM combines PACE and Chip Authentication 1 for faster execution times. Hence, a TOE meeting the original requirement also meets the refined requirement.

67. Application note (taken from [5], application note 28)

The SFR FIA_UAU.5.1/PACE_EAC1PP in the current ST covers the definition in [13] and extends it by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE_EAC1PP in the current ST covers the definition in [13] and extends it by EAC aspects 2), 3), 4) and 5). These extensions do not conflict with the strict conformance to [13].

FIA_UAU.6/EAC_EAC1PP
Re-authenticating – Re-authenticating of Terminal by the TOE

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.[135]

[132] [selection: *the Authentication Mechanism with Personalisation Agent Key(s)*]
[133] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
[134] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
[135] [assignment: *list of conditions under which re-authentication is required*]

68. Application note (taken from [5], application note 29)

The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [8] 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 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
Authentication Proof of Identity

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 [16][136] to prove the identity of the TOE.[137]

69. Application note (taken from [5], application note 30)

This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [16]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or ECDH) and two session keys for secure messaging in ENC_MAC mode according to [8]. The terminal verifies by means of secure messaging whether the electronic 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).

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

FIA_API.1.1/PACE_CAM

The TSF shall provide a protocol PACE-CAM [9][138] to prove the identity of the TOE.[139]

[136] [assignment: *authentication mechanism*]
[137] [assignment: *authorized user or role*]
[138] [assignment: *authentication mechanism*]
[139] [assignment: *authorized user or role, or of the TOE itself*]

The following SFR is newly defined in this ST and addresses the Active Authentication protocol:

FIA_API.1/AA
Authentication Proof of Identity

Hierarchical to: No other components

Dependencies: No dependencies

FIA_API.1.1/AA

The TSF shall provide a Active Authentication protocol according to [7] [9][140] to prove the identity of the TOE.[141]

The following SFRs are imported due to claiming [14]. They concern access mechanisms for an eSign application, if available.

- **FIA_UID.1/SSCDPP**
- **FIA_AFL.1/SSCDPP**

FIA_UID.1/SSCDPP
Timing of identification

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**~~ **FPT_TST.1/SSCDPP**,
2. none[142]

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

FIA_UID.1.2/SSCDPP

[140] [assignment: *authentication mechanism*]
[141] [assignment: *authorized user or role, or of the TOE itself*]
[142] [assignment: *list of additional 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.

70. Application note (taken from [14], application note 11)

Applied.

71. Application note (from ST author)

The refinement was necessary to ensure unified terminology usage of SFRs.

FIA_AFL.1/SSCDPP
Authentication failure handling

Hierarchical to:	No other components
Dependencies:	FIA_UAU.1 Timing of Authentication fulfilled by FIA_UAU.1/SSCDPP

FIA_AFL.1.1/SSCDPP

The TSF shall detect when an administrator configurable positive integer within 3-15[143] unsuccessful authentication attempts occur related to consecutive failed authentication attempts.[144]

FIA_AFL.1.2/SSCDPP

When the defined number of unsuccessful authentication attempts has been met[145], the TSF shall block RAD[146].

72. Application note (taken from [14], application note 13)

Applied

6.1.2.3. *SFRs for eSign-applications*

FIA_UAU.1/SSCDPP
Timing of authentication

Hierarchical to:	No other components

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

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

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

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

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/SSCD**~~ **FPT_TST.1/SSCDPP**,
2. identification of the user by means of TSF required by ~~**FIA_UID.1/SSCD**~~ **FIA_UID.1/SSCDPP**,
3. establishing a trusted channel between CGA and the TOE by means of TSF required by ~~**FPT_ITC.1/CA_EAC2**~~ **FTP_ITC.1/CA_EAC2PP**,
4. establishing a trusted channel between HID and the TOE by means of TSF required by ~~**FPT_ITC.1/CA_EAC2**~~ **FTP_ITC.1/CA_EAC2PP**,
5. none[147]

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.

73. Application note (from ST author)

The refinement was necessary to ensure unified terminology usage of SFRs.

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 [5] and FDP_ACF.1/EAC2PP from [6] are unified in [20] to one single FDP_ACF.1/TRM, whereas the several iterations of FDP_ACF.1 from [14] stand separate. [20] takes 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, how FDP_ACF.1/EAC1PP is covered as well is explained.

[147] [assignment: *list of additional TSF-mediated actions*]

Concerning FDP_ACF.1/TRM in [20] and the several iterations FDP_ACF.1 from [14], [20] remarks 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 [14] apply, an EAC2 terminal and the Electronic Document Holder need to be authenticated. Hence, no inconsistency exists.

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

Hierarchical to:	No other components
Dependencies:	FDP_ACC.1 Subset access control fulfilled by FDP_ACC.1/TRM_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[148] to objects based on the following:

1) Subjects:
   a) Terminal,
   b) PACE terminal,
   c) EAC2 terminal Authentication Terminal and Signature Terminal according to [17][149],
   d) EAC1 terminal;[150]
2) Objects:

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

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

[150] [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 [6]*)

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).[151][152]

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 [17] **and/or [7]**, ~~as~~ required by ~~**FIA_UAU.1/PACE**~~ **FIA_UAU.1/PACE_EAC2PP or FIA_UAU.1/PACE_EAC1PP**.[153]

FDP_ACF.1.3/TRM

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.[154]

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.[155]
2. Terminals not using secure messaging are not allowed to read, write, modify, or use any data stored on the electronic document.

[151] [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 [6]*)

[152] [*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. [2]*)

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

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

[155] note that authentication of an EAC1 or EAC2 terminal to a TOE in certified mode implies a prior run of PACE.

3. No subject is allowed to read ‘Electronic Document 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:
    1. CAN change
    2. Change PIN
    3. Resume PIN
    4. Unblock PIN
    5. Activate PIN
    6. Deactivate PIN according to [17].[156]
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~~ **FIA_UAU.5/PACE_EAC2PP**) to determine access rights of the terminal according to [17]. 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/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~~ **FIA_UAU.1/PACE_EAC1PP**, 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. [16] and [8].

[156] [assignment*: list of rules for PIN management chosen from [17]*]

9. If Sensitive User Data is protected both by EAC1 and EAC2, no subject is allowed to read those data except EAC1 terminals or 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).[157]

74. Application note (from ST author)

The [20] uses the ‘Electronic Document Communication Establishment Authorization Data’ expression in 3.1.1.2 Secondary Assets and “Communication Establishment Authorization Data” in FDP_ACF.1.4/TRM 3. In order to provide consistency in our ST, we use only the Electronic Document Communication Establishment Authorization Data.

75. Application note (taken from [20], application note 11)

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 [17]. However the references are compatible as justified in [6], yet both are mentioned here since [17] is the primary norm for an eID application, whereas [7] 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 [6] that definitions in [17] and [8] are compatible.

FDP_ACF.1.3/TRM is taken over from [5] and [6] (same formulation in both).

Rules 1 and 2 of FDP_ACF.1.4/TRM_EAC1PP in [5] 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 [5] are combined here to rule 8, where terminals need the corresponding CHAT to read data groups. Rule 5 of [5] is here equivalent to rule 7. None of this conflict with strict conformance to [5]. 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

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

refinement. Since the protection level and mechanisms w.r.t. to EAC2-protected data do not change, strict conformance is not violated.

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 [6]. None of these 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 [5] applies the assignment operation, whereas in [6] (by referencing [13]) 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.

76. Application note (from ST author)

The refinements were necessary to ensure unified terminology usage of SFRs.

The following SFRs are imported due to claiming [6]. 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 75. Application note (taken from [20], application note 11).

- **FDP_ACF.1/TRM_EAC2PP**

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

- **FDP_RIP.1/EAC2PP**
- **FDP_UCT.1/TRM_EAC2PP**
- **FDP_UIT.1/TRM_EAC2PP**

FDP_ACC.1/TRM_EAC2PP
Subset access control – Terminal Access

Hierarchical to:	No other components
Dependencies:	FDP_ACF.1 Security attribute based access control: fulfilled by FDP_ACF.1/TRM

FDP_ACC.1.1/TRM_EAC2PP

The TSF shall enforce the Access Control SFP[158] on terminals gaining access to the User Data stored in the ~~**travel document**~~ **electronic document**[159] and none[160].

77. Application note (taken from [20])

This SFR is equivalent to/covered by FDP_ACC.1/TRM_EAC1PP; cf.75. Application note (taken from [20], application note 11).

78. Application note (from ST author)

The refinement was necessary to ensure unified terminology usage as described in Table 1 Overview of identifiers of current ST and PPs.

FDP_RIP.1/EAC2PP
Subset residual information protection

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[161] the following objects:

1. Session keys **(PACE-K_{MAC}, PACE-K_{Enc}), (CA2-K_{MAC}, CA2-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)[162],
4. none.[163]

79. Application note (taken from [6], application note 30)

The functional family FDP_RIP possesses such a general character, 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/EAC2PP requires a certain quality metric (*any previous information content of a resource is made*

[158] [assignment: *access control SFP*]
[159] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[160] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[161] [selection: *allocation of the resource to, deallocation of the resource from*]
[162] [assignment: *list of objects*]
[163] [assignment: *list of objects*]

unavailable) for key destruction in addition to FCS_CKM.4/EAC2PP that merely requires to ensure key destruction according to a method/standard.

Application note 80 (from ST author)

The above SFR is slightly refined from [20] in order not to confuse Chip Authentication 1 with Chip Authentication 2.

FDP_UCT.1/TRM_EAC2PP
Basic data exchange confidentiality – MRTD

Hierarchical to: No other components

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] fulfilled by FTP_ITC.1/PACE_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_EAC2PP

The TSF shall enforce the Access Control SFP[164] to be able to transmit and receive[165] user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/TRM_EAC2PP
TRM Data exchange integrity

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[166] to be able to transmit and receive[167] user data in a manner protected from modification, deletion, insertion and replay[168] errors.

[164] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[165] [selection: *transmit, receive*]
[166] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[167] [selection: *transmit, receive*]
[168] [selection: *modification, deletion, insertion, replay*]

FDP_UIT.1.2/TRM_EAC2PP

The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[169] has occurred.

The following SFRs are imported due to claiming [5]. They concern access control mechanisms related to EAC1-protected data.

- **FDP_ACC.1/TRM_EAC1PP**

The above is equivalent **FDP_ACC.1/TRM_EAC2PP**, since EF.SOD (cf. FDP_ACC.1/TRM in [5]) 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**
- **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)

FDP_RIP.1/EAC1PP
Subset residual information protection

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[170] the following objects:

1. Session Keys (immediately after closing related communication session) ,

[169] [selection: *modification, deletion, insertion, replay*]
[170] [selection: *allocation of the resource to, deallocation of the resource from*]

2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret K[171]).[172]
3. none.[173]

The following SFRs are imported due to claiming [14]. They concern access control mechanisms of an eSign application.

- **FDP_ACC.1/SCD/SVD_Generation_SSCDPP**
- **FDP_ACF.1/SCD/SVD_Generation_SSCDPP**
- **FDP_ACC.1/SVD_Transfer_SSCDPP**
- **FDP_ACF.1/SVD_Transfer_SSCDPP**
- **FDP_ACC.1/Signature-creation_SSCDPP**
- **FDP_ACF.1/Signature-creation_SSCDPP**
- **FDP_RIP.1/SSCDPP**
- **FDP_SDI.2/Persistent_SSCDPP**
- **FDP_SDI.2/DTBS_SSCDPP**

FDP_ACC.1/SCD/SVD_Generation_SSCDPP
Subset access control

Hierarchical to: No other components

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

FDP_ACC.1.1/SCD/SVD_Generation_SSCDPP

The TSF shall enforce the SCD/SVD Generation SFP[174] on

1. subjects: S.User,
2. objects: SCD, SVD,
3. operations: generation of SCD/SVD pair. [175]

FDP_ACF.1/SCD/SVD_Generation_SSCDPP
Security attribute based access control

[171] according to [7]
[172] [assignment: *list of objects*]
[173] [assignment: *list of objects*]
[174] [assignment: *access control SFP*]
[175] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

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 initialisation fulfilled by FMT_MSA.3/SSCDPP

FDP_ACF.1.1/SCD/SVD_Generation_SSCDPP

The TSF shall enforce the SCD/SVD Generation SFP[176] to objects based on the following: the user S.User is associated with the security attribute "SCD/SVD Management".[177]

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.[178]

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.[179]

FDP_ACF.1.4/SCD/SVD_Generation_SSCDPP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.[180]

FDP_ACC.1/SVD_Transfer_SSCDPP Subset access control

Hierarchical to: No other components

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

[177] [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*]

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

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

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

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

FDP_ACC.1.1/SVD_Transfer_SSCDPP

The TSF shall enforce the SVD Transfer SFP[181] on

1. subjects: S.User,
2. objects: SVD
3. operations: export.[182]

FDP_ACF.1/SVD_Transfer_SSCDPP Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control fulfilled by FDP_ACC.1/SVD_Transfer_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[183] to objects based on the following:

1. the S.User is associated with the security attribute Role,
2. the SVD.[184]

FDP_ACF.1.2/SVD_Transfer_SSCDPP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Admin[185] is allowed to export SVD.[186]

FDP_ACF.1.3/SVD_Transfer_SSCDPP

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

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

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

[184] [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*]

[185] [selection:_*R.Admin, R.Sigy*]

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

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.[187]

FDP_ACF.1.4/SVD_Transfer_SSCDPP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.[188]

81. Application note (taken from [14], application note 9)

Applied.

FDP_ACC.1/Signature-creation_SSCDPP Subset access control

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

The TSF shall enforce the Signature Creation SFP[189] on

1. subjects: S.User,
2. objects: DTBS/R, SCD,
3. operations: signature creation.[190]

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

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/Signature_Creation_SSCDPP

[187] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[188] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[189] [assignment: *access control SFP*]
[190] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

The TSF shall enforce the Signature Creation SFP[191] to objects based on the following:

1. the user S.User is associated with the security attribute “Role” and
2. the SCD with the security attribute “SCD Operational”.[192]

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 electronic signatures for DTBS/R with SCD which security attribute “SCD operational” is set to “yes”.[193]

FDP_ACF.1.3/Signature_Creation_SSCDPP

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.[194]

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 electronic signatures for DTBS/R with SCD which security attribute “SCD operational” is set to “no”.[195]

FDP_RIP.1/SSCDPP
Subset residual information protection

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[196] the following objects: SCD[197].

[191] [assignment: *access control SFP*]
[192] [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*]
[193] [assignment*: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[194] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[195] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[196] [selection: *allocation of the resource to, deallocation of the resource from*]
[197] [assignment: *list of objects*]

FDP_SDI.2/Persistent_SSCDPP Stored data integrity monitoring and action

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[198] on all objects, based on the following attributes: integrity checked stored data[199].

FDP_SDI.2.2/Persistent_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.[200]

82. Application note (taken from [14])

The [14] was defined the followings:

The following data persistently stored by the TOE shall have the user data attribute "integrity checked persistent stored data":

1) SCD
2) SVD (if persistently stored by the TOE).

The DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data"

FDP_SDI.2/DTBS_SSCDPP Stored data integrity monitoring and action

Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies

FDP_SDI.2.1/DTBS_SSCDPP

[198] [assignment: *integrity errors*]
[199] [assignment: *user data attributes*]
[200] [assignment: *action to be taken*]

The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[201] on all objects, based on the following attributes: integrity checked stored DTBS.[202]

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.[203]

83. Application note (taken from [14], application note 10)

The integrity of TSF data like RAD shall be protected to ensure the effectiveness of the user authentication. This protection is a specific aspect of the security architecture (cf. ADV_ARC.1).

6.1.4. Class FTP

The following SFRs are imported from [6].

- **FTP_ITC.1/PACE_EAC2PP**
- **FTP_ITC.1/CA_EAC2PP**

FTP_ITC.1/PACE_EAC2PP
Inter-TSF trusted channel after PACE

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 [17]**.

FTP_ITC.1.2/PACE_EAC2PP

[201] [assignment: *list of objects*]
[202] [assignment: *user data attributes*]
[203] [assignment: *action to be taken*]

The TSF shall permit ~~another trusted IT product~~ **a PACE terminal**[204] 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**.[205]

84. Application note (taken from [6], application note 31)

The above definition refines FTP_ITC.1 from [13]. The definitions there are unclear as to what the "other trusted IT product" actually is. Since we distinguish here between trusted channels that are established once after PACE, and then then (re)established after CA2, the above refinement is necessary for clarification.

FTP_ITC.1/CA_EAC2PP
Inter-TSF trusted channel after CA2

Hierarchical to:	No other components
Dependencies:	No dependencies

FTP_ITC.1.1/CA2_EAC2PP

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 [17]**.

FTP_ITC.1.2/CA2_EAC2PP

The TSF shall permit ~~another trusted IT product~~ **an EAC2 terminal**[206] to initiate communication via the trusted channel.

FTP_ITC.1.3/CA2_EAC2PP

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.[207]

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

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

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

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

85. Application note (taken from [6], application note 32)

The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE_EAC2PP), the TA2 protocol (FIA_UAU.1/EAC2_Terminal_EAC2PP) and the CA2 protocol (FIA_API.1/CA_EAC2PP). If Chip Authentication 2 was successfully performed, secure messaging is immediately restarted using the derived session keys (CA-K_{MAC}, CA-K_{Enc})[208]. This secure messaging enforces the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC_EAC2PP and FCS_COP.1/PACE_MAC_EAC2PP.

The following SFR is imported due to claiming [5]. It concerns applications with EAC1-protected data.

- **FTP_ITC.1/PACE_EAC1PP**

FTP_ITC.1/PACE_EAC1PP
Inter-TSF trusted channel after PACE

Hierarchical to: No other components

Dependencies: No dependencies

FTP_ITC.1.1/PACE_EAC1PP

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/PACE_EAC1PP

The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE_EAC1PP

The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Terminal.[209]

[208] otherwise secure messaging is continued using the established PACE session keys, cf. FTP_ITC.1/PACE_EAC1PP

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

6.1.5. Class FAU

The following SFR is imported due to claiming [6]. It concerns applications with EAC2-protected data.

- **FAU_SAS.1/EAC2PP**

FAU_SAS.1/EAC2PP
Audit storage

Hierarchical to:	No other components
Dependencies:	No dependencies

FAU_SAS.1.1_EAC2PP

The TSF shall provide the Manufacturer[210] with the capability to store the Initialisation and Pre-Personalisation Data[211] in the audit records.

The following SFR is imported due to claiming [5]. 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)

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

FMT_SMR.1.1

[210] [assignment: *authorised users*]
[211] [assignment: *list of management functions to be provided by the TSF*]

The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Country Verifying Certification Authority (CVCA),
4. Document Verifier (DV),
5. Terminal,
6. PACE Terminal,
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.[212]

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

The next SFRs are imported from [6]. They concern mainly applications with EAC2-protected data.

- **FMT_MTD.1/CVCA_INI_EAC2PP**
- **FMT_MTD.1/CVCA_UPD_EAC2PP**
- **FMT_SMF.1/EAC2PP**
- **FMT_SMR.1/PACE_EAC2PP**

This SFR is combined with FMT_SMR.1/PACE_EAC1PP into to by **FMT_SMR.1**.

- **FMT_MTD.1/DATE_EAC2PP**
- **FMT_MTD.1/PA_EAC2PP**
- **FMT_MTD.1/SK_PICC_EAC2PP**
- **FMT_MTD.1/KEY_READ_EAC2PP**
- **FMT_MTD.1/Initialize_PIN_EAC2PP**
- **FMT_MTD.1/Change_PIN_EAC2PP**
- **FMT_MTD.1/Resume_PIN_EAC2PP**
- **FMT_MTD.1/Unblock_PIN_EAC2PP**
- **FMT_MTD.1/Activate_PIN_EAC2PP**
- **FMT_MTD.3/EAC2PP**

[212] [assignment: *the authorized identified roles*]

- **FMT_LIM.1/EAC2PP**

86. Application note (taken from [20], application note 12)

The above SFR concerns the whole TOE, not just applications with EAC2-protected data.

- **FMT_LIM.2/EAC2PP**

87. Application note (taken from [20], application note 13)

The above SFR concerns the whole TOE, not just applications with EAC2-protected data.

- **FMT_MTD.1/INI_ENA_EAC2PP**
- **FMT_MTD.1/INI_DIS_EAC2PP**

FMT_MTD.1/CVCA_INI_EAC2PP
Management of TSF data – Initialization of CVCA Certificate and Current Date

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/ EAC2PP

FMT_MTD.1.1/CVCA_INI_EAC2PP

The TSF shall restrict the ability to write[213] the

1. initial CVCA Public Key ,
2. meta-data of the initial CVCA Certificate as required in [17], resp. [18],
3. initial Current Date,
4. none[214]

to the Personalization Agent.[215][216].

88. Application note (taken from [6], application note 36)

[213] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[214] [assignment: *list of TSF data*]
[215] [assignment: *the authorized identified roles*]
[216] [selection: *the manufacturer, the personalization agent*]

The initial CVCA Public Key may be written by the manufacturer in the manufacturing phase or by the Personalization Agent in the issuing phase (cf. [17]). The initial CVCA Public Keys and their updates later on are used to verify the CVCA Link-Certificates.

FMT_MTD.1/CVCA_UPD_EAC2PP Management of TSF data – Country Verifying Certification Authority

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/CVCA_UPD_EAC2PP

The TSF shall restrict the ability to update[217] the

1. CVCA Public Key (PK_{CVCA}),
2. meta-data of the CVCA Certificate as required by [17], resp. [18],[218]
3. none[219]

to the Country Verifying Certification Authority.[220]

89. Application note (taken from [6], application note 37)

The CVCA updates its asymmetric key pair and distributes the public key and related meta-data by means of CVCA Link-Certificates. The TOE updates its internal trust-point, if a valid CVCA Link-Certificate (cf. FMT_MTD.3/EAC2PP) is provided by the terminal (cf. [18]).

FMT_SMF.1/EAC2PP Specification of Management Functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1/EAC2PP

The TSF shall be capable of performing the following management functions:

[217] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[218] [assignment: *list of TSF data*]
[219] [assignment: *list of TSF data*]
[220] [assignment: *the authorized identified roles*]

1. Initialization,
2. Pre-Personalization,
3. Personalization,
4. Configuration,
5. **Resume and unblock the PIN (if any),**
6. **Activate and deactivate the PIN (if any).**[221]

90. Application note (taken from [6], application note 33)

The capability of PIN management gives additional security to the TOE.

91. Application note (taken from [6], application note 34)

The SFR is here refined by including mechanisms for PIN management. A TOE without PIN management functionality can only use a commonly shared secret (such as the MRZ – in the case of an ID document – or the CAN) during execution of PACE to control access to sensitive information. A PIN however must not be shared and thus can be kept secret by the user. Hence, this refinement of FMT_SMF.1/EAC2PP increases protection of user data by allowing PIN access, and thus does not violate strict conformity to [13].

FMT_MTD.1/DATE_EAC2PP
Management of TSF data – Current date

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_EAC2PP

The TSF shall restrict the ability to modify[222] the current date[223] to

1. CVCA,
2. Document Verifier,
3. EAC2 terminal (Authentication Terminal and Signature Terminal[224]) possessing an Accurate Terminal Certificate according to [18].[225]

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

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

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

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

[225] [assignment: *the authorized identified roles*]

4. none[226]

92. Application note (taken from [6], application note 38)

The authorized roles are identified in their certificates (cf. [17]) and are authorized by validating the certificate chain up to the CVCA (cf. FMT_MTD.3/EAC2PP). The authorized role of a terminal is part of the Certificate Holder Authorization in the card verifiable certificate that is provided by the terminal within Terminal Authentication 2 (cf. [18]). Different types of EAC2 terminals may exist, cf. [17].

FMT_MTD.1/PA_EAC2PP
Management of TSF data – Personalization Agent

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[227] the **card/chip security object(s) (SO_C) and the document Security Object (SO_D)**[228] to the Personalization Agent[229].

93. Application note (taken from [6], application note 39)

Note that the card/chip security objects are mentioned here as well. These contain information, such as algorithm identifiers, only necessary for EAC2. All requirements formulated in [13] are thus met, and strict conformance is therefore not violated

FMT_MTD.1/SK_PICC_EAC2PP
Management of TSF data – Chip Authentication and Restricted Identification Private Key(s)

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

[226] [assignment: *the authorized identified roles*]
[227] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[228] [assignment: *list of TSF data*]
[229] [assignment: *the authorized identified roles*]

FMT_MTD.1.1/SK_PICC_EAC2PP

The TSF shall restrict the ability to create or load[230][231] the Chip Authentication private key(s) (SK_{PICC}) and the Restricted Identification Private Key(s)[232] to the Personalization Agent **or the Manufacturer**.[233]

94. Application note (taken from [6], application note 40)

Applied, see FCS_CKM.1/CA2 and FCS_CKM.1/RI.

95. Application note (from ST author)

The **FMT_MTD.1/SK_PICC_EAC2PP** was refined, because the Manufactuer means here the electronic document manufacturer, which may create the application and the file system as well. So the Manufacturer may generate or load the private keys.

FMT_MTD.1/KEY_READ_EAC2PP
Management of TSF data – Private Key Read

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[234] the

1. PACE passwords,
2. Personalization Agent Keys,
3. the Chip Authentication private key(s) (SK_{PICC})
4. the Restricted Identification private key(s)[235]
5. none[236]

[230] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[231] [selection*: create, load*]
[232] [assignment: *list of TSF data*]
[233] [assignment: *the authorized identified roles*]
[234] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[235] [assignment: *list of TSF data*]
[236] [assignment: *list of TSF data]*

to none[237]

96. Application note (taken from [6], application note 41)

FMT_MTD.1/KEY_READ_EAC2PP extends the SFR from [13] by additional assignments.

FMT_MTD.1/Initialize_PIN_EAC2PP
PIN Management of TSF data – Initialize PIN

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[238] the initial PIN and PUK[239] to the Personalization Agent[240]

FMT_MTD.1/Change_PIN_EAC2PP
Management of TSF data – Changing PIN

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/Change_PIN_EAC2PP

The TSF shall restrict the ability to change[241] the blocked PIN[242] to

1. Electronic Document Holder (using the PUK) with unauthenticated terminal

[237] [assignment: *the authorized identified roles*]
[238] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[239] [assignment: *list of TSF data*]
[240] [assignment: *the authorized identified roles*]
[241] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[242] [assignment: *list of TSF data*]

2. Authentication Terminal with the Terminal Authorisation level for PIN management according to [17].[243][244]

FMT_MTD.1/Resume_PIN_EAC2PP
Management of TSF data – Resuming PIN

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[245] the suspended PIN[246] to the Electronic Document Holder[247]

97. Application note (taken from [6], application note 42)

Resuming is a two-step procedure, subsequently using PACE with the CAN and PACE with the PIN. It must be implemented according to [17], and is relevant for the status as required by FIA_AFL.1/Suspend_PIN_EAC2PP. The Electronic Document Holder is authenticated as required by FIA_UAU.1/PACE_EAC2PP using the PIN as the shared password.

FMT_MTD.1/Unblock_PIN_EAC2PP
Management of TSF data – Unblocking PIN

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

[243] [assignment: *the authorized identified roles*]
[244] [assignment: *the authorised identified roles that match the list of PIN changing rules conformant to [17]*]
[245] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[246] [assignment: *list of TSF data*]
[247] [assignment: *the authorized identified roles*]

The TSF shall restrict the ability to unblock[248] the blocked PIN[249] 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.[250]

98. Application note (taken from [6], application note 43)

The unblocking procedure must be implemented according to [17], and is relevant for the status as required by FIA_AFL.1/Block_PIN_EAC2PP. It can be triggered by either (i) the Electronic Document Holder being authenticated as required by FIA_UAU.1/PACE_EAC2PP using the PUK as the shared password or (ii) an EAC2 terminal (FIA_UAU.1/EAC2_Terminal_EAC2PP) that proved a terminal authorization level being sufficient for PIN management (FDP_ACF.1/TRM).

FMT_MTD.1/Activate_PIN_EAC2PP
Management of TSF data – Activating/Deactivating PIN

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[251] the PIN[252] to an EAC2 terminal of a type that has the terminal authorization level for PIN management[253].

99. Application note (taken from [6], application note 44)

The activation/deactivation procedures must be implemented according to [17]. They can be triggered by an EAC2 terminal (FIA_UAU.1/EAC2_Terminal_EAC2PP) that proved a terminal authorization level sufficient for PIN management (FDP_ACF.1/TRM).

FMT_MTD.3/EAC2PP
Secure TSF data

Hierarchical to:	No other components

[248] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[249] [assignment: *list of TSF data*]
[250] [assignment: *the authorized identified roles*]
[251] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[252] [assignment: *list of TSF data*]
[253] [assignment: *the authorized identified roles*]

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[254]. **Refinement: To determine if the certificate chain is valid, the TOE shall proceed the certificate validation according to [18].**

100. Application note (taken from [6], application note 45)

Terminal Authentication is used as required by (i) FIA_UID.1/EAC2_Terminal_EAC2PP and FIA_UAU.5/PACE_EAC2PP. The terminal authorization level derived from the CVCA Certificate, the DV Certificate and the Terminal Certificate is used as TSF-data for the access control required by FDP_ACF.1/TRM.

In addition, this ST contains all remaining SFRs of the claimed [13].

FMT_LIM.1/EAC2PP
Limited capabilities

Hierarchical to: No other components

Dependencies: FMT_LIM.2 Limited availability: fulfilled by FMT_LIM.2/EAC2PP

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. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks.[255] and

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

[255] [assignment: *Limited capability and availability policy*]

5. EAC1 and EAC2 protected data[256]

Application note 101 (from ST author)

The assignment was necessary to cover all protected user data.

FMT_LIM.2/EAC2PP
Limited availability

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. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks.[257] and
5. EAC1 and EAC2 protected data[258]

Application note 102 (from ST author)

The assignment was necessary to cover all protected user data.

FMT_MTD.1/INI_ENA_EAC2PP
Management of TSF data – Writing Initialisation and Pre-personalisation Data

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1/EAC2PP

[256] [assignment: *Limited capability and availability policy*]
[257] [assignment: *Limited capability and availability policy*]
[258] [assignment: *Limited capability and availability policy*]

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[259] the Initialisation Data and Pre-personalisation Data[260] to the Manufacturer.[261]

FMT_MTD.1/INI_DIS_EAC2PP Management of TSF data – Reading and Using Initialisation and Pre-personalisation Data

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[262] the Initialisation Data and the Pre-personalisation Data[263] to the Personalisation Agent.[264]

The following SFRs are imported due to claiming [5]. They mainly concern applications with EAC1-protected data.

- **FMT_SMF.1/EAC1PP**
- **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.

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

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

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

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

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

[264] [assignment: *the authorized identified roles*]

- **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 **FMT_MTD.1/INI_ENA_EAC2PP**, but listed here for the sake of completeness)

- **FMT_MTD.1/INI_DIS_EAC1PP**

(equivalent to **FMT_MTD.1/INI_DIS_EAC2PP**, but listed here for the sake of completeness)

- **FMT_MTD.1/CVCA_INI_EAC1PP**
- **FMT_MTD.1/CVCA_UPD_EAC1PP**
- **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 [5].

- **FMT_MTD.1/CAPK_EAC1PP**
- **FMT_MTD.1/PA_EAC1PP**
- **FMT_MTD.1/KEY_READ_EAC1PP**
- **FMT_MTD.3/EAC1PP**

FMT_SMF.1/EAC1PP
Specification of Management Functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1/EAC1PP

The TSF shall be capable of performing the following management functions:

1. Initialization,
2. Pre-personalisation,
3. Personalisation

4. Configuration.[265]

FMT_MTD.1/CVCA_INI_EAC1PP
Management of TSF data – Initialization of CVCA Certificate and Current Date

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

The TSF shall restrict the ability to write[266] the

1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifying Certification Authority Certificate,
3. initial Current Date,
4. none[267][268]

to Personalisation Agent[269].

103. Application note (taken from [5], application note 41)

Applied.

FMT_MTD.1/CVCA_UPD_EAC1PP
Management of TSF data – Country Verifying Certification Authority

Hierarchical to:	No other components
Dependencies:	FMT_SMF.1 Specification of management functions functions fulfilled by FMT_SMF.1/EAC1PP
	FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/PACE_EAC1PP

[265] [assignment: *list of management functions to be provided by the TSF*]
[266] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[267] [assignment: *list of TSF data*]
[268] [assignment: *list of TSF data*]
[269] [assignment: *the authorised identified roles*]

FMT_MTD.1.1/CVCA_UPD_EAC1PP

The TSF shall restrict the ability to update[270] the

1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate[271]

to Country Verifying Certification Authority.[272]

104. Application note (taken from [5], application note 42)

The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates (cf. [16]). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3/EAC1PP) is provided by the terminal (cf. [16])

FMT_MTD.1/CAPK_EAC1PP
Management of TSF data – Chip Authentication Private Key

Hierarchical to:	No other components
Dependencies:	FMT_SMF.1 Specification of management functions functions fulfilled by FMT_SMF.1/EAC1PP
	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 create, load[273][274] the Chip Authentication Private Key[275] to Manufacturer or Personalisation Agent.[276]

105. Application note (taken from [5], application note 44)

Applied.

FMT_MTD.1/PA_EAC1PP
Management of TSF data – Personalisation Agent

[270] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[271] [assignment: *list of TSF data*]
[272] [assignment: *the authorised identified roles*]
[273] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[274] [selection: *create, load*]
[275] [assignment: *list of TSF data*]
[276] [assignment: *the authorisedidentified roles*]

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/PA_EAC1PP

The TSF shall restrict the ability to write[277] the Document Security Object (SO_D)[278] to the Personalisation Agent.[279]

FMT_MTD.1/KEY_READ_EAC1PP Management of TSF data – Key Read

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_EAC1PPFMT_MTD.1.1/KEY_READ_EAC1PP

The TSF shall restrict the ability to read[280] the

1. PACE passwords,
2. Chip Authentication Private Key,
3. Personalisation Agent Keys[281]
4. **Active Authentication Private Key**

to none[282]

106. Application note (taken from [5], application note 45)

[277] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[278] [assignment: *list of TSF data*]
[279] [assignment: *the authorised identified roles*]
[280] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[281] [assignment: *list of TSF data*]
[282] [assignment: *the authorised identified roles*]

The SFR FMT_MTD.1/KEY_READ_EAC1PP in the ST covers the definition in [13] and extends it by additional TSF data. This extension does not conflict with the strict conformance to [13].

107. Application note (ST author)

The refinement was necessary because of the Active Authentication protocol.

FMT_MTD.3/EAC1PP
Secure TSF data

Hierarchical to:	No other components
Dependencies:	FMT_MTD.1 Management of TSF data fulfilled by FMT_MTD.1/CVCA_INI_EAC1PP and FMT_MTD.1/CVCA_UPD_EAC1PP

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.[283]

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.**

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

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~~ EAC1 terminal**.**

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~~ EAC1 terminal**.**

108. Application note (taken from [5], application note 46)

The Terminal Authentication Version 1 is used for EAC1 terminal as required by FIA_UAU.4/PACE_EAC1PP and FIA_UAU.5/PACE_EAC1PP. 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 [14]. They mostly concern the security management of an *eSign* application.

- **FMT_SMR.1/SSCDPP**
- **FMT_SMF.1/SSCDPP**
- **FMT_MOF.1/SSCDPP**
- **FMT_MSA.1/Admin_SSCDPP**
- **FMT_MSA.1/SignatorySSCDPP**
- **FMT_MSA.2/SSCDPP**
- **FMT_MSA.3/SSCDPP**
- **FMT_MSA.4/SSCDPP**
- **FMT_MTD.1/Admin_SSCDPP**
- **FMT_MTD.1/Signatory_SSCDPP**

FMT_SMR.1/SSCDPP
Security roles

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[284]

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

FMT_SMR.1.2/SSCDPP

The TSF shall be able to associate users with roles.

FMT_SMF.1/SSCDPP
Security Management Functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1/SSCDPP

The TSF shall be capable of performing the following 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, [285]
5. Unblock the RAD[286]

109. Application note (taken from [14], application note 14)

Applied.

FMT_MOF.1/SSCDPP
Management of security functions behaviour

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_MOF.1.1/SSCDPP

The TSF shall restrict the ability to enable[287] the functions signature creation function[288] to R.Sigy[289].

[285] [assignment: *list of other security management functions to be provided by the TSF*]
[286] [assignment: *list of other security management functions to be provided by the TSF*]
[287] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
[288] [assignment: *list of functions*]
[289] [assignment: *the authorised identified roles*]

FMT_MSA.1/Admin_SSCDPP Management Security attributes

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[290] to restrict the ability to modify, none[291] the security attributes SCD/SVD management[292] to R.Admin[293].

FMT_MSA.1/SignatorySSCDPP Management Security attributes

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/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

[290] [assignment: access control SFP(s), information flow control SFP(s)]

[291] [assignment: *other operations*]

[292] [assignment: *list of security attributes*]

[293] [assignment: *the authorized identified roles*]

The TSF shall enforce the SCD/SVD Generation SFP[294] to restrict the ability to modify[295] the security attributes SCD operational[296] to R.Sigy[297].

FMT_MSA.2/SSCDPP
Secure security attributes

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 and FDP_ACC.1/Signature-creation_SSCDPP
	FMT_MSA.1 Management of security attributes fulfilled by FMT_MSA.1/Admin_SSCDPP and FMT_MSA.1/SignatorySSCDPP.
	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[298].

110. Application note (taken from [14], application note 15)

Applied.

FMT_MSA.3/SSCDPP
Static attribute initialisation

Hierarchical to:	No other components
Dependencies:	FMT_MSA.1 Management of security attributes fulfilled by FMT_MSA.1/Admin_SSCDPP and FMT_MSA.1/SignatorySSCDPP.

[294] [assignment: *access control SFP(s), information flow control SFP(s)*]
[295] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[296] [assignment: *list of security attributes*]
[297] [assignment: *the authorized identified roles*]
[298] [selection: *list of security attributes*]

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[299] to provide restrictive[300] default values for security attributes that are used to enforce SFP.

FMT_MSA.3.2/ SSCDPP

The TSF shall allow the R.Admin[301] to specify alternative initial values to override the default values when an object or information created.

FMT_MSA.4/SSCDPP Security attribute value inharitance

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 and FDP_ACC.1/Signature-creation_SSCDPP

FMT_MSA.4/SSCDPP

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.[302]

111. Application note (taken from [14], application note 16)

The TOE may not support generating an SVD/SCD pair by the signatory alone, in which case rule (2) is not relevant.

[299] [assignment: *access control SFP, information flow control SFP*]

[300] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

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

[302] [assignment: *rules for setting the values of security attributes*]

FMT_MTD.1/Admin_SSCDPP
Management of TSF data

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[303] the RAD[304] to R.Admin[305].

FMT_MTD.1/Signatory_SSCDPP
Management of TSF data

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[306],none[307] the RAD[308] to R.Sigy[309].

112. Application note (taken from [14], application note 17)

Applied.

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

[303] [selection: *change_default, query, modify, delete, clear, [assignment: other operations*]
[304] [assignment: *list of TSF data*]
[305] [assignment: *the authorised identified roles*]
[306] [selection: *change_default, query, modify, delete, clear, [assignment: other operations*]
[307] [selection: *change_default, query, modify, delete, clear, [assignment: other operations*]
[308] [assignment: *list of TSF data*]
[309] [assignment: *the authorised identified roles*]

Hierarchical to: No other components

Dependencies: FMT_ LIM.2 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 the locking of the Loader[310] does not allow stored user data to be disclosed or manipulated by unauthorized users.[311]

113. Application note (taken from [20], application note 14)

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 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 the locking of the Loader[312][313]

114. Application note (taken from [20], application note 15)

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 SFR is new and concern security management for ePassport application in combination with [5] in case the Active Authentication protocol is active:

[310] [assignment: *action*]
[311] [assignment: *Limited capability and availability policy*]
[312] [assignment: *action*]
[313] [assignment: *Limited capability and availability policy*]

FMT_MTD.1/AA_Private_Key
Management of TSF data – Active Authentication Private Key

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/AA_Private_Key

The TSF shall restrict the ability to create or load[314] the Active Authentication Private Key[315] to the Personalization Agent.[316]

6.1.7. Class FPT

The following security functional requirements are imported from [6], and address the protection against forced illicit information leakage, including physical manipulation.

- **FPT_EMS.1/EAC2PP**

115. Application note (taken from [20], application note 16)

Note that related to Application Note 6 of [20], 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.

- **FPT_FLS.1/EAC2PP**
- **FPT_TST.1/EAC2PP**
- **FPT_PHP.3/EAC2PP**

The following SFRs are imported due to claiming [5]. 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)

[314] [assignment: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[315] [assignment: *list of TSF data*]
[316] [assignment: *the authorized identified roles*]

- **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**

The following SFRs are imported due to claiming [14]. They mostly concern the protection of security functionality related to eSign application (if available).

- **FPT_EMS.1/SSCDPP**
- **FPT_FLS.1/SSCDPP**

(subsumed by **FPT_FLS.1/EAC2PP**)

- **FPT_PHP.1/SSCDPP**
- **FPT_PHP.3/SSCDPP**

(subsumed by **FPT_PHP.3/EAC2PP**)

- **FPT_TST.1/SSCDPP**

(subsumed by **FPT_TST.1/EAC2PP**)

FPT_EMS.1/EAC2PP
TOE Emanation

Hierarchical to:	No other components
Dependencies:	No dependencies

FPT_EMS.1.1/EAC2PP

The TOE shall not emit variations in power consumption or timing during command execution[317] in excess of non-useful information[318] enabling access to

1. **the** session keys (PACE-K_{MAC}, PACE-K_{Enc}), **(CA-K_{MAC}, CA-K_{Enc}),**

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

[318] [assignment: *specified limits*]

2. the ephemeral private key ephem-SK_{PICC}-PACE, [319]
3. the Chip Authentication private keys (SK_{PICC})
4. the PIN, PUK,
5. none[320]

and

6. the Restricted Identification private key(s) SK_{ID}, [321]
7. none.[322]

FPT_EMS.1.2/EAC2PP

The TSF shall ensure any users[323] are unable to use the following interface electronic document's contactless/contact-based interface and circuit contacts[324] to gain access to

1. the session keys (PACE-K_{MAC}, PACE-K_{Enc}), **(CA2-K_{MAC}, CA2-K_{Enc}),**
2. the ephemeral private key ephem -SK_{PICC}-PACE1,
3. the Chip Authentication private key(s) (SK_{PICC}),
4. the PIN, PUK,
5. ~~**the session keys (PACE-K_{MAC}, PACE-K_{Enc}), (CA-K_{MAC}, CA-K_{Enc})**~~**[325]**
6. none[326]

and

7. the Restricted Identification private key(s) SK_{ID},[327]
8. none.[328]

116. Application note (taken from [6], application note 46)

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

[319] [assignment: *list of types of TSF data*]
[320] [assignment: *list of types of TSF data*]
[321] [assignment: *list of types of user data*]
[322] [assignment: *list of types of user data*]
[323] [assignment: *type of users*]
[324] [assignment: *type of connection*]
[325] [assignment: *list of types of TSF data*]
[326] [assignment: *list of types of TSF data*]
[327] [assignment: *list of types of user data*]
[328] [assignment: *list of types of user data*]

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/EAC2PP 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.

Note that in the above SFR, all items in FPT_EMS.1/EAC2PP from 3. upwards are additional assignments. The first item is slightly refined to include CA-key(s).

117. Application note (from ST author)

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 [6] by adding all relevant key material from Chip Authentication 2, 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 [6]. Hence, the requirement is stricter than the one from [6], and the refinement operation is justified.

The FPT_EMS.1.2/EAC2PP is refined because in the [20] first and fifth point is identical and unnecessary to repeat the first point in the current ST.

FPT_FLS.1/EAC2PP
Failure with preservation of secure state

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,[329]
3. none.[330]

FPT_TST.1/EAC2PP
TSF testing

Hierarchical to:	No other components
Dependencies:	No dependencies

FPT_TST.1.1/EAC2PP

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

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

The TSF shall run a suite of self tests during initial start-up, periodically during normal operation[331]to demonstrate the correct operation of the TSF.[332]

FPT_TST.1.2/EAC2PP

The TSF shall provide authorised users with the capability to verify the integrity of the TSF data.[333]

FPT_TST.1.3/EAC2PP

The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.[334]

FPT_PHP.3/EAC2PP
Resistance to physical attack

Hierarchical to: No other components

Dependencies: No dependencies

FPT_PHP.3.1_EAC2PP

The TSF shall resist physical manipulation and physical probing[335] to the TSF[336] by responding automatically such that the SFRs are always enforced.

FPT_EMS.1/EAC1PP
TOE Emanation

Hierarchical to: No other components

Dependencies: No dependencies

FPT_EMS.1.1/EAC1PP

The TOE shall not emit variations in power consumption or timing during command execution[337] in excess of non-useful information[338] enabling access to

1. Chip Authentication **(Version 1)** Session Keys,

[331] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]*]
[332] [selection: *[assignment: parts of TSF], the TSF*]
[333] [selection: *[assignment: parts of TSF], TSF data*]
[334] [selection: *[assignment: parts of TSF], TSF*]
[335] [assignment: *physical tampering scenarios*]
[336] [assignment: *list of TSF devices/elements*]
[337] [assignment: *types of emissions*]
[338] [assignment: *specified limits*]

2. PACE session Keys (PACE-K_{MAC}, PACE-K_{Enc}),
3. the ephemeral private key ephem SK_{PICC}-PACE,
4. the ephemeral private key $SK_{MapPICC}$-PACE-CAM[339]
5. Active Authentication Private Key[340]
6. Personalisation Agent Key(s)
7. Chip Authentication **(Version 1)** Private Key [341] and
8. none [342]

FPT_EMS.1.2/EAC1PP

The TSF shall ensure any users[343] are unable to use the following interface smart card circuit contacts[344] 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 $SK_{MapPICC}$-PACE-CAM[345]
5. Active Authentication Private Key[346]
6. Personalisation Agent Key(s)
7. Chip Authentication **(Version 1)** Private Key [347] and
8. none.[348]

118. Application note (from ST author)

This SFR covers the definition of FPT_EMS.1 in [5] and extends it by 4. and 5. of FPT_EMS.1.1/EAC1PP and FPT_EMS.1.2/EAC1PP. Also, 1. and 7. of both FPT_EMS.1.1/EAC1PP and FPT_EMS.1.2/EAC1PP are slightly refined in order not to confuse Chip Authentication 1 with Chip Authentication 2.

Note that FPT_EMS.1/EAC1PP in [5] 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 $SK_{Map,PICC}$-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

[339] [assignment: *list of types of TSF data*]
[340] [assignment: *list of types of TSF data*]
[341] [assignment: *list of types of user data*]
[342] [assignment: *list of types of user data*]
[343] [assignment: *type of users*]
[344] [assignment: *type of connection*]
[345] [assignment: *list of types of TSF data*]
[346] [assignment: *list of types of TSF data*]
[347] [assignment: *list of types of TSF data*]
[348] [assignment: *list of types of user data*]

of the ephemeral key $SK_{Map,PICC}$-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 $CA_{PICC} = SK_{Map,PICC}$-PACE-CAM ° i($SK_{PICC}$) to the terminal, a malicious attacker that gains knowledge of $SK_{Map,PICC}$-PACE-CAM can reveal SK_{PICC} by computing SK_{PICC} = i(CA_{PICC}) ° $SK_{Map,PICC}$-PACE-CAM.

Because of the Active Authentication is supported protocol by the TOE, the SFR is extended with Active Authentication Private Key.

119. Application note (taken from[5], application note 48)

Applied.

FPT_EMS.1/SSCDPP
TOE Emanation

Hierarchical to: No other components

Dependencies: No dependencies

FPT_EMS.1.1_SSCD

The TOE shall not emit emit variations in power consumption or timing during command execution[349] in excess of non-useful information[350] enabling access to RAD[351] and SCD[352].

FPT_EMS.1.2_SSCD

The TSF shall ensure that unauthorized[353] are unable to use the following interface electrical contacts[354] to gain access to RAD[355] and SCD[356].

120. Application note (taken from [14], application note 18)

The TOE shall prevent attacks against the SCD and other 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 or may origin from internal operation of the TOE or may origin 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 TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.

[349] [assignment: *types of emissions*]
[350] [assignment: *specified limits*]
[351] [assignment: *list of types of TSF data*]
[352] [assignment: *list of types of user data*]
[353] [assignment: *type of users*]
[354] [assignment: *type of connection*]
[355] [assignment: *list of types of TSF data*]
[356] [assignment: *list of types of user data*]

Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

FPT_PHP.1/SSCDPP
Passive detection of physical attack

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.

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).

3696 6.3.Security Requirements Rationale

3697 6.3.1. Security Functional Requirements Rationale

3698 The following table provides an overview for the coverage of the security functional requirements, and also gives evidence for sufficiency and
3699 necessity of the chosen SFRs.

	OT.CA2	OT.Chip_Auth_Proof[5]	OT.Chip_Auth_Proof_PACE_CAM	OT.Chip_Auth_Proof_AA	OT.Sens_Data_Conf [5]	OT.AC_Pers_EAC2	OT.Sens_Data_EAC2	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.AC_Pers	OT.Prot_Inf_Leak	OT.RI_EAC2	OT.Non_Interfere	OT.SCD/SVD_Gen [14]	OT.Sigy_SigF ([14])	OT.Cap_Avail_Loader
Class FCS																		
FCS_CKM.1/CAM	-	-	X	-	-	-	-	X	X	X	-	-	-	-	-	-	-	-
FCS_COP.1/CAM	-	-	X	-	-	-	-	X	X	X	-	-	-	-	-	-	-	-
FCS_CKM.1/CA2	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
FCS_CKM.1/RI	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	-
FCS_CKM.1/AA	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-
FCS_COP.1/AA	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Class FIA																		
FIA_UID.1/PACE_EAC1PP	-	-	X	-	X	-	-	X	X	X	-	X	-	-	-	-	-	-
FIA_UAU.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	

	OT.CA2	OT.Chip_Auth_Proof[5]	OT.Chip_Auth_Proof_PACE_CAM	OT.Chip_Auth_Proof_AA	OT.Sens_Data_Conf [5]	OT.AC_Pers_EAC2	OT.Sens_Data_EAC2	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.AC_Pers	OT.Prot_Inf_Leak	OT.RI_EAC2	OT.Non_Interfere	OT.SCD/SVD_Gen [14]	OT.Sigy_SigF ([14])	OT.Cap_Avail_Loader
FIA_UAU.4/PACE_EAC1PP	-	-	-	X	-	-	-	X	X	X	-	-	-	-	-	-	-	-
FIA_API.1/AA	-	-	-	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
FMT_MTD.1/KEY_READ_EAC1PP	-	X	-	X	X	-	-	X	X	X	-	X	-	-	-	-	-	-
FMT_MTD.1/AA_Private_Key	-	-	X		-	-	-	-	-	-	-	X	-	-	-	-	-	-
Class FPT																		
FPT_EMS.1/EAC1PP	-	-	-	-	-	-	-	-	-	-	-	X	X	-	X	-	-	-
FPT_EMS.1/EAC2PP	-	-	-	-	-	X	-	-	-	-	-	-	X	-	X	-	-	-
FPT_EMS.1/SSCDPP	-	-	-	-	-	-		-	-	-	-	-	-	-	X	-	-	-

3700 Table 11 Coverage of Security Objectives for the TOE by SFRs

According to [1], 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 or [20] by checking the rows of Table 11 , 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 or [20] by checking the non-cursive columns of Table 11 , and for the other security objectives by looking up the rationale of that PP.

In other words, in Table 11 , we list only:

- SFRs that have been newly added or refined within this ST or [20]. 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 or [20], and their related SFRs.
- Security objectives for the TOE that are affected by the above newly added or refined SFRs.

In case an SFR was refined in order to ensure the unified terminology usage, those SFRs are not listed in Table 11 or justifies below, because these refinements have no security impacts.

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 [5], [6] and [14].

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.Chip_Auth_Proof_AA is a newly introduced security objective that aims to ensure the authenticity of the electronic document’s chip by the Active Authentication protocol, in particular in the context of an ePassport Application. This is supported by **FCS_CKM.1/AA** for cryptographic key generation, and **FIA_API.1/AA, FIA_UAU.4/PACE_EAC1PP** and **FCS_COP.1/AA** for the implementation itself. The **FMT_MTD.1/KEY_READ_EAC1PP** ensures the authenticity of the TOE, because it restricts the ability to read the Active Authentication private key to none. These do not affect the discussion of the rationale of [5].

The OT.AC_Pers enforce that all TSF data can be written by authorized Personalisation Agent only and this is supported by **FMT_MTD.1/AA_Private_Key** for the Active Authentication key pair.

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 [14].

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 [5] and [6] 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 [5] and [6].

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 [5] and [6] 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.

The security objective **OT.CA2** aims at enabling verification of the authenticity of the TOE as a whole device. This objective is mainly achieved as described in [20]. The secure generation of cryptography key pair is ensured by **FCS_CKM.1/CA2**.

The security objective **OT.RI_EAC2** aims at providing a way to pseudonymously identify an electronic document holder without granting a terminal read access to sensitive user data. This objective is mainly achieved as described in [20]. The secure generation of cryptography key pair is ensured by **FCS_CKM.1/RI**.

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 [2] 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, through 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 the current ST.

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 components, 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.1

fulfilled 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.1

fulfilled 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.

7. TOE Summary Specification

7.1.TOE Security Functions

7.1.1. TSF.AccessControl

The TOE enforces access control in order to access User Data and TSF-data and maintains different security roles.

SFR	Description
FIA_AFL.1/Suspend_PIN_EAC2PP	The TSF responsible to suspend the reference value of PIN.
FIA_AFL.1/Block_PIN_EAC2PP	The TSF responsible to block the reference value of PIN.
FIA_AFL.1/SSCDPP	The TSF responsible to block the reference value of RAD.
FIA_UID.1/PACE_EAC2PP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user identification.
FIA_UID.1/EAC2_Terminal_EAC2PP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user identification.
FIA_UAU.1/PACE_EAC2PP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user authentication.
FIA_UAU.1/EAC2_Terminal_EAC2PP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user authentication.
FIA_AFL.1/PACE_EAC2PP	The TSF responsible to delay each following authentication attempt.
FIA_UID.1/PACE_EAC1PP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user identification.
FIA_UAU.1/PACE_EAC1PP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user authentication.
FIA_AFL.1/PACE_EAC1PP	Equivalent to FIA_AFL.1/PACE_EAC2PP.
FIA_UID.1/SSCDPP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user identification.
FIA_UAU.1/SSCDPP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user authentication.
FDP_ACC.1/TRM_EAC2PP	This TSF responsible to enforce the Access Control SFP.
FDP_ACF.1/TRM	This TSF responsible to enforce the Access Control SFP.
FDP_ACC.1/TRM_EAC1PP	Equivalent to FDP_ACC.1/TRM_EAC2PP.
FDP_ACC.1/SCD/SVD_Generation_SSCDPP	This TSF responsible to enforce the SCD/SVD Generation SFP.
FDP_ACF.1/SCD/SVD_Generation_SSCDPP	This TSF responsible to enforce the SCD/SVD Generation SFP.
FDP_ACC.1/SVD_Transfer_SSCDPP	This TSF responsible to enforce the SVD Transfer SFP.
FDP_ACF.1/SVD_Transfer_SSCDPP	This TSF responsible to enforce the SVD Transfer SFP.
FDP_ACC.1/Signature-creation_SSCDPP	This TSF responsible to enforce the Signature Creation SFP.

FDP_ACF.1/Signature-creation_SSCDPP	This TSF responsible to enforce the Signature Creation SFP.
FMT_MTD.1/CVCA_INI_EAC2PP	This TSF responsible to restrict the ability to write certain objects.
FMT_MTD.1/CVCA_UPD_EAC2PP	This TSF responsible to restrict the ability to update certain objects.
FMT_MTD.1/DATE_EAC2PP	This TSF responsible to restrict the ability to modify the current date.
FMT_MTD.1/PA_EAC2PP	This TSF responsible to restrict the ability to write certain objects.
FMT_MTD.1/SK_PICC_EAC2PP	This TSF responsible to restrict the ability to create or load the Chip Authentication private key(s) (SKPICC) and the Restricted Identification Private Key(s).
FMT_MTD.1/KEY_READ_EAC2PP	This TSF responsible to restrict the ability to read certain objects.
FMT_SMR.1	This TSF responsible to maintain the Manufacturer, Personalization Agent, Country Verifying Certification Authority (CVCA), Document Verifier (DV), Terminal, PACE Terminal, EAC2 terminal, if the eID, ePassport and/or eSign application are active, EAC1 terminal, if the ePassport application is active, Electronic Document Holder roles.
FMT_SMR.1/SSCDPP	This TSF responsible to maintain the R.Admin and R.Sigy roles.
FMT_MOF.1/SSCDPP	This TSF responsible to restrict the ability to enable the functions signature creation function.
FMT_MSA.1/Admin_SSCDPP	This TSF responsible to enforce the SCD/SVD Generation SFP.
FMT_MSA.1/SignatorySSCDPP	This TSF responsible to enforce the SCD/SVD Generation SFP.
FMT_MSA.3/SSCDPP	This TSF responsible to enforce the SCD/SVD Generation SFP, SVD Transfer SFP and Signature Creation SFP.
FMT_MTD.1/Admin_SSCDPP	This TSF responsible to restrict the ability to create the RAD.
FMT_MTD.1/Signatory_SSCDPP	This TSF responsible to restrict the ability to modify the RAD
FMT_MTD.1/CVCA_INI_EAC1PP	This TSF responsible to shall restrict the ability to write certain objects.
FMT_MTD.1/CVCA_UPD_EAC1PP	This TSF responsible to restrict the ability to update certain objects.
FMT_MTD.1/DATE_EAC1PP	This TSF responsible to restrict the ability to modify the current date.
FMT_MTD.1/CAPK_EAC1PP	This TSF responsible to restrict the ability to create, load the Chip Authentication Private Key.
FMT_MTD.1/PA_EAC1PP	This TSF responsible to restrict the ability to write the Document Security Object (SOD).
FMT_MTD.1/KEY_READ_EAC1PP	This TSF responsible to restrict the ability to read certain objects.
FMT_MTD.1/AA_Private_Key	This TSF responsible to restrict the ability to create or load the Active Authentication Private Key.

7.1.2. TSF.Authenticate

The TOE supports several authentication mechanism in order to authenticate the Users, Terminals and to prove the genuineness of the electronic document.

The supported mechanism and protocols are based on ICAO and BSI standards [7], [8], [16], [17] and [18].

Supported authentication mechanism:

- Password Authenticated Connection Establishment (PACE) [7], [16], [17].
  - Generic Mapping
  - Chip Authentication Mapping
- Active Authentication [7]
- Chip Authentication version 1 [16]
- Terminal Authentication version 1 [16]
- Chip Authentication version 2 [17]
- Terminal Authentication version 2 [17]
- Restricted Identification [17]
- Symmetric Authentication (Device authentication) [30]
- Symmetric Role Authentication [30]
- User Verification [30]

SFR	Description
FIA_AFL.1/Suspend_PIN_EAC2PP	This TSF responsible for PACE.
FIA_AFL.1/Block_PIN_EAC2PP	This TSF responsible for PACE.
FIA_API.1/CA_EAC2PP	This TSF responsible for Chip Authentication v2.
FIA_API.1/RI_EAC2PP	This TSF responsible for Restricted Identification.
FIA_UID.1/PACE_EAC2PP	This TSF responsible for PACE.
FIA_UID.1/EAC2_Terminal_EAC2PP	This TSF responsible for PACE.
FIA_UAU.1/PACE_EAC2PP	This TSF responsible for PACE.
FIA_UAU.1/EAC2_Terminal_EAC2PP	This TSF responsible for PACE and Terminal Authentication v2.
FIA_UAU.4/PACE_EAC2PP	This TSF responsible for PACE, Terminal Authentication v2 and Symmetric Authentication.
FIA_UAU.5/PACE_EAC2PP	This TSF responsible for PACE, Terminal Authentication v2, Chip Authentication v2 and Symmetric Authentication.
FIA_UAU.6/CA_EAC2PP	This TSF responsible for Chip Authentication v2.
FIA_AFL.1/PACE_EAC2PP	This TSF responsible for PACE.
FIA_UAU.6/PACE_EAC2PP	This TSF responsible for PACE.
FIA_UID.1/PACE_EAC1PP	This TSF responsible for PACE, Chip Authentication v1 and Chip Authentication Mapping (PACE-CAM).
FIA_UAU.1/PACE_EAC1PP	This TSF responsible for PACE, Chip Authentication v1, Terminal Authentication v1 and Chip Authentication Mapping (PACE-CAM).
FIA_UAU.4/PACE_EAC1PP	This TSF responsible for PACE, Symmetric Authentication, Terminal Authentication v1 and Active Authentication.
FIA_UAU.5/PACE_EAC1PP	This TSF responsible for PACE, Chip Authentication Mapping (PACE-CAM), Symmetric Authentication, Terminal Authentication v1.
FIA_UAU.6/EAC_EAC1PP	This TSF responsible for Chip Authentication v1
FIA_API.1/EAC1PP	This TSF responsible for Chip Authentication v1
FIA_API.1/PACE_CAM	This TSF responsible for Chip Authentication Mapping
FIA_API.1/AA	This TSF responsible for Active Authentication
FIA_AFL.1/PACE_EAC1PP	Equivalent to FIA_AFL.1/PACE_EAC2PP.
FIA_UAU.6/PACE_EAC1PP	This TSF responsible for PACE.
FIA_AFL.1/SSCDPP	This TSF responsible for User Verification.
FDP_ACF.1/TRM	This TSF responsible for Terminal Authentication and PACE.
FDP_ACF.1/SCD/SVD_Generation_SSCDPP	This TSF responsible for User Verification

FDP_ACF.1/SVD_Transfer_SSCDPP	This TSF responsible for R.Admin.
FDP_ACF.1/Signature-creation_SSCDPP	This TSF responsible for User Verification.
FTP_ITC.1/PACE_EAC2PP	This TSF responsible for PACE
FTP_ITC.1/CA_EAC2PP	This TSF responsible for Chip Authentication v2
FTP_ITC.1/PACE_EAC1PP	This TSF responsible for PACE.
FMT_MTD.1/CVCA_INI_EAC2PP	This TSF responsible for authentication of the Personalisation Agent.
FMT_MTD.1/CVCA_UPD_EAC2PP	This TSF responsible for the authentication of Country Verifying Certification Authority.
FMT_MTD.1/DATE_EAC2PP	This TSF responsible for the authentication of CVCA, DV and the EAC2 Terminal
FMT_MTD.1/PA_EAC2PP	This TSF responsible for authentication of Personalization Agent.
FMT_MTD.1/SK_PICC_EAC2PP	This TSF responsible for authentication of the Personalisation Agent.
FMT_MTD.1/Initialize_PIN_EAC2PP	This TSF responsible for authentication of the Personalisation Agent.
FMT_MTD.1/Change_PIN_EAC2PP	This TSF responsible for authentication of Document Holder and the EAC2 Terminal (with Terminal Authorisation level for PIN management).
FMT_MTD.1/Resume_PIN_EAC2PP	This TSF responsible for authentication of Document Holder
FMT_MTD.1/Unblock_PIN_EAC2PP	This TSF responsible for authentication of Document Holder and the EAC2 Terminal (with Terminal Authorisation level for PIN management).
FMT_MTD.1/Activate_PIN_EAC2PP	This TSF responsible for authentication of the EAC2 Terminal (with Terminal Authorisation level for PIN management).
FMT_MTD.3/EAC2PP	This TSF responsible for the Terminal Authentication v2.
FMT_SMF.1/SSCDPP	This TSF responsible to provide the security functions.
FMT_MOF.1/SSCDPP	This TSF responsible for authentication of R.Sigy
FMT_MSA.1/Admin_SSCDPP	This TSF responsible for authentication of R.Admin
FMT_MSA.1/SignatorySSCDPP	This TSF responsible for authentication of R.Sigy
FMT_MSA.3/SSCDPP	This TSF responsible for authentication of R.Sigy and R.Admin
FMT_MSA.4/SSCDPP	This TSF responsible for authentication of R.Sigy and R.Admin
FMT_MTD.1/Admin_SSCDPP	This TSF responsible for authentication of R.Admin
FMT_MTD.1/Signatory_SSCDPP	This TSF responsible for authentication of R.Sigy
FMT_MTD.1/CVCA_INI_EAC1PP	This TSF responsible for authentication of Personalization Agent.
FMT_MTD.1/CVCA_UPD_EAC1PP	This TSF responsible for authentication of Country Verifying Certification Authority.
FMT_MTD.1/DATE_EAC1PP	This TSF responsible to equivalent to FMT_MTD.1/DATE_EAC2PP.
FMT_MTD.1/CAPK_EAC1PP	This TSF responsible for This TSF responsible for authentication of Personalization Agent or the Manufacturer.
FMT_MTD.1/PA_EAC1PP	This TSF responsible for authentication of Personalization Agent.
FMT_MTD.1/AA_Private_Key	This TSF responsible for authentication of Personalization Agent.
FMT_MTD.3/EAC1PP	This TSF responsible for the Terminal Authentication v2.

7.1.3. TSF.SecureManagement

The TOE enforces the secure management of the security attributes, data and functions. Furthermore the TOE restricts the available commands in each TOE life-cycle phase.

SFR	Description
FMT_MTD.1/CVCA_INI_EAC2PP	This TSF responsible to evaluate whether the Personalisation Agent is authenticated, and it has right to write initial CVCA Public Key, meta-data of the initial CVCA Certificate and initial Current Date.
FMT_MTD.1/CVCA_UPD_EAC2PP	This TSF responsible to evaluate whether the Country Verifying Certification Authority is authenticated, and it has right to update CVCA Public Key (PKCVCA) and meta-data of the CVCA Certificate.
FMT_SMF.1/EAC2PP	This TSF responsible to provide part of the security functions.
FMT_MTD.1/DATE_EAC2PP	This TSF responsible to evaluate whether a CVCA, Document Verifier, or an EAC2 terminal is authenticated and it has right to modify Current Date.
FMT_MTD.1/PA_EAC2PP	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to write the card/chip security object(s) (SO_C) and the document Security Object (SO_D).
FMT_MTD.1/SK_PICC_EAC2PP	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to create or load the Chip Authentication private key(s) (SKPICC) and the Restricted Identification Private Key(s).
FMT_MTD.1/KEY_READ_EAC2PP	This TSF responsible to restrict the ability to read certain objects.
FMT_MTD.1/Initialize_PIN_EAC2PP	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to write the initial PIN and PUK
FMT_MTD.1/Change_PIN_EAC2PP	This TSF responsible to evaluate whether an Electronic Document Holder is authenticated with PUK or a Terminal with Terminal Authorisation level for PIN management is authenticated and it has right to change the blocked PIN.
FMT_MTD.1/Resume_PIN_EAC2PP	This TSF responsible to evaluate whether an Electronic Document Holder is authenticated, and it has right to resume the suspended PIN.
FMT_MTD.1/Unblock_PIN_EAC2PP	This TSF responsible to evaluate whether an Electronic Document Holder is authenticated with PUK or a Terminal with Terminal Authorisation level for PIN management is authenticated and it has right to unblock the blocked PIN.
FMT_MTD.1/Activate_PIN_EAC2PP	This TSF responsible to evaluate whether a Terminal with Terminal Authorisation level for PIN management is authenticated and it has right to activate or deactivate the PIN.
FMT_SMF.1/SSCDPP	This TSF responsible to provide part of the security functions.
FMT_MOF.1/SSCDPP	This TSF responsible to evaluate whether a R.Sigy is authenticated and it has right to enable the signature creation function.
FMT_MSA.1/Admin_SSCDPP	This TSF responsible to evaluate whether a R.Admin is authenticated and it has right to modify the SCD/SVD management security attribute.

FMT_MSA.1/SignatorySSCDPP	This TSF responsible to evaluate whether a R.Sigy is authenticated and it has right to modify the SCD/SVD operational security attribute.
FMT_MSA.2/SSCDPP	This TSF responsible to ensure that only secure values are accepted for SCD/SVD Management and SCD operational
FMT_MSA.3/SSCDPP	This TSF responsible to provide restrictive default values for security attributes.
FMT_MSA.4/SSCDPP	This TSF responsible for security attribute value inheritance.
FMT_MTD.1/Admin_SSCDPP	This TSF responsible to evaluate whether a R.Admin is authenticated, and it has right to create the RAD.
FMT_MTD.1/Signatory_SSCDPP	This TSF responsible to evaluate whether a R.Sigy is authenticated and it has right to modify the RAD.
FMT_MTD.1/CVCA_INI_EAC1PP	This TSF responsible to evaluate whether the Personalisation Agent is authenticated, and it has right to write initial Country Verifying Certification Authority Public Key, initial Country Verifying Certification Authority Certificate, initial Current Date.
FMT_MTD.1/CVCA_UPD_EAC1PP	This TSF responsible to evaluate whether the Country Verifying Certification Authority is authenticated, and it has right to update Country Verifying Certification Authority Public Key, Country Verifying Certification Authority Certificate.
FMT_SMF.1/EAC1PP	This TSF responsible to provide part of the security functions.
FMT_MTD.1/DATE_EAC1PP	This TSF responsible to equivalent to FMT_MTD.1/DATE_EAC2PP.
FMT_MTD.1/CAPK_EAC1PP	This TSF responsible to evaluate whether a Personalisation Agent or Manufacturer is authenticated, and it has right to create or load the Chip Authentication private key.
FMT_MTD.1/PA_EAC1PP	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to write the document Security Object (SOD).
FMT_MTD.1/KEY_READ_EAC1PP	This TSF responsible to restrict the ability to read cryptographic keys.
FMT_MTD.1/AA_Private_Key	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to create or load the Active Authentication Private Key.

7.1.4. TSF.CryptoKey

The TOE uses several cryptographic services such as digital signature creation and verification, asymmetric and symmetric cryptography, random number generation and complete key management.

Furthermore TSF.CryptoKey provides the secure messaging for the TOE.

SFR	Description
FCS_CKM.1/DH_PACE_EAC2PP	This TSF responsible the Applet part of key agreement for PACE.
FCS_COP.1/SHA_EAC2PP	This TSF responsible the Applet part of hash generation.
FCS_COP.1/SIG_VER_EAC2PP	This TSF responsible the Applet part of digital signature verification.
FCS_COP.1/PACE_ENC_EAC2PP	This TSF responsible the Applet part of secure messaging – encryption and decryption.
FCS_COP.1/PACE_MAC_EAC2PP	This TSF responsible the Applet part of secure messaging – message authentication code.

FCS_CKM.4/EAC2PP	This TSF responsible the Applet part of cryptographic key destruction.
FCS_RND.1/EAC2PP	This TSF responsible the Applet part of random number generation.
FCS_CKM.1/DH_PACE_EAC1PP	This TSF responsible the Applet part of key agreement for PACE.
FCS_CKM.4/EAC1PP	Equivalent to FCS_CKM.4/EAC2PP.
FCS_COP.1/PACE_ENC_EAC1PP	This TSF responsible the Applet part of secure messaging – encryption and decryption.
FCS_COP.1/PACE_MAC_EAC1PP	This TSF responsible the Applet part of secure messaging – message authentication code.
FCS_RND.1/EAC1PP	Equivalent to FCS_RND.1/EAC2PP.
FCS_CKM.1/CA_EAC1PP	This TSF responsible the Applet part of key agreement for Chip Authentication v1.
FCS_COP.1/CA_ENC_EAC1PP	This TSF responsible the Applet part of secure messaging – encryption and decryption.
FCS_COP.1/SIG_VER_EAC1PP	This TSF responsible the Applet part of digital signature verification.
FCS_COP.1/CA_MAC_EAC1PP	This TSF responsible the Applet part of secure messaging – message authentication code.
FCS_CKM.1/CA2	This TSF responsible the Applet part of Chip Authentication version 2 Key pair(s) generation.
FCS_CKM.1/RI	This TSF responsible the Applet part of Restricted Identification Key pair (s) generation.
FCS_CKM.1/AA	This TSF responsible the Applet part of Active Authentication Key Pair generation.
FCS_COP.1/AA	This TSF responsible the Applet part of digital signature generation.
FCS_CKM.1/CAM	This TSF responsible the Applet part of PACE-CAM protocol implementation.
FCS_COP.1/CAM	This TSF responsible the Applet part of PACE-CAM protocol implementation.
FCS_CKM.1/SSCDPP	This TSF responsible the Applet part of SCD/SVD pair generation.
FCS_COP.1/SSCDPP	This TSF responsible the Applet part of digital signature creation.
FIA_API.1/CA_EAC2PP	This TSF responsible the Applet part of cryptographic operation for Chip Authentication v2.
FIA_API.1/RI_EAC2PP	This TSF responsible the Applet part of cryptographic operation for Restricted Identification.
FIA_API.1/EAC1PP	This TSF responsible the Applet part of cryptographic operation for Chip Authentication v1.
FIA_API.1/PACE_CAM	This TSF responsible the Applet part of cryptographic operation for Chip Authentication Mapping.
FIA_API.1/AA	This TSF responsible the Applet part of cryptographic operation for Active Authentication.
FDP_RIP.1/EAC2PP	This TSF responsible to call the Platform functionalities to destroy cryptographic keys.
FDP_UCT.1/TRM_EAC2PP	This TSF responsible the Applet part of secure messaging.
FDP_UIT.1/TRM_EAC2PP	This TSF responsible the Applet part of secure messaging.
FDP_RIP.1/EAC1PP	This TSF responsible to call the Platform functionalities to destroy cryptographic keys.
FDP_UCT.1/TRM_EAC1PP	Equivalent to FDP_UCT.1/TRM_EAC2PP.
FDP_UIT.1/TRM_EAC1PP	Equivalent to FDP_UIT.1/TRM_EAC2PP.
FDP_RIP.1/SSCDPP	This TSF responsible the Applet part of de-allocation of the resource SCD.
FTP_ITC.1/PACE_EAC2PP	This TSF responsible the Applet part of cryptographic operation for trusted channel.

FTP_ITC.1/CA_EAC2PP	This TSF responsible the Applet part of cryptographic operation for trusted channel.
FTP_ITC.1/PACE_EAC1PP	This TSF responsible the Applet part of cryptographic operation for trusted channel.

7.1.5. TSF.AppletParametersSign

The TOE enforces the integrity of itself in each life cycle phases.

SFR	Description
FPT_TST.1/EAC2PP	This TSF responsible for initial start-up, periodically during normal operation testing.
FPT_TST.1/EAC1PP	Equivalent to FPT_TST.1/EAC2PP.
FPT_TST.1/SSCDPP	Subsumed by FPT_TST.1/EAC2PP.

7.1.6. TSF.Platform

The TOE relies on the certified functions and services of the Platform. This TSF is collection of those SFRs, which are uses these functions and services.

SFR	Description
FCS_CKM.1/DH_PACE_EAC2PP	This TSF responsible the Platform part of key agreement for PACE.
FCS_COP.1/SHA_EAC2PP	This TSF responsible the Platform part of hash generation.
FCS_COP.1/SIG_VER_EAC2PP	This TSF responsible the Platform part of digital signature verification.
FCS_COP.1/PACE_ENC_EAC2PP	This TSF responsible the Platform part of secure messaging – encryption and decryption.
FCS_COP.1/PACE_MAC_EAC2PP	This TSF responsible the Platform part of secure messaging – message authentication code.
FCS_CKM.4/EAC2PP	This TSF responsible the Platform part of cryptographic key destruction.
FCS_RND.1/EAC2PP	This TSF responsible the Platform part of random number generation.
FCS_CKM.1/DH_PACE_EAC1PP	This TSF responsible the Platform part of key agreement for PACE.
FCS_CKM.4/EAC1PP	Equivalent to FCS_CKM.4/EAC2PP.
FCS_COP.1/PACE_ENC_EAC1PP	This TSF responsible the Platform part of secure messaging – encryption and decryption.
FCS_COP.1/PACE_MAC_EAC1PP	This TSF responsible the Platform part of secure messaging – message authentication code.
FCS_RND.1/EAC1PP	Equivalent to FCS_RND.1/EAC2PP.
FCS_CKM.1/CA_EAC1PP	This TSF responsible the Platform part of key agreement for Chip Authentication v1.
FCS_COP.1/CA_ENC_EAC1PP	This TSF responsible the Platform part of secure messaging – encryption and decryption.
FCS_COP.1/SIG_VER_EAC1PP	This TSF responsible the Platform part of digital signature verification.
FCS_COP.1/CA_MAC_EAC1PP	This TSF responsible the Platform part of secure messaging – message authentication code.
FCS_CKM.1/CA2	This TSF responsible the Platform part of Chip Authentication version 2 Key pair(s) generation.
FCS_CKM.1/RI	This TSF responsible the Platform part of Restricted Identification Key pair(s) generation.
FCS_CKM.1/AA	This TSF responsible the Platform part of Active Authentication Key Pair generation.

FCS_COP.1/AA	This TSF responsible the Platform part of digital signature generation.
FCS_CKM.1/CAM	This TSF responsible the Platform part of PACE-CAM protocol implementation.
FCS_COP.1/CAM	This TSF responsible the Platform part of PACE-CAM protocol implementation.
FCS_CKM.1/SSCDPP	This TSF responsible the Platform part of SCD/SVD pair generation.
FCS_CKM.4/SSCDPP	This TSF responsible the Platform part of cryptographic key destruction.
FCS_COP.1/SSCDPP	This TSF responsible the Platform part of digital signature creation.
FIA_API.1/CA_EAC2PP	This TSF responsible the Platform part of cryptographic operation for Chip Authentication v2.
FIA_API.1/RI_EAC2PP	This TSF responsible the Platform part of cryptographic operation for Restricted Identification.
FIA_UID.1/PACE_EAC2PP	This TSF responsible for the identifier data of the TOE.
FIA_UID.1/EAC2_Terminal_EAC2PP	This TSF responsible for the identifier data of the TOE.
FIA_UAU.1/PACE_EAC2PP	This TSF responsible for the identifier data of the TOE.
FIA_UAU.1/EAC2_Terminal_EAC2PP	This TSF responsible for the identifier data of the TOE.
FIA_UID.1/PACE_EAC1PP	This TSF responsible for the identifier data of the TOE.
FIA_UAU.1/PACE_EAC1PP	This TSF responsible for the identifier data of the TOE.
FIA_UAU.4/PACE_EAC2PP	This TSF responsible for fresh random numbers for PACE, Terminal Authentication v2 and Symmetric Authentication.
FIA_UAU.5/PACE_EAC2PP	This TSF responsible for Platform part of cryptographic operation for PACE, Terminal Authentication v2, Chip Authentication v2 and Symmetric Authentication.
FIA_UAU.6/CA_EAC2PP	This TSF responsible for Platform part of cryptographic operation for Chip Authentication v2.
FIA_UAU.6/PACE_EAC2PP	This TSF responsible for Platform part of cryptographic operation for PACE.
FIA_UAU.4/PACE_EAC1PP	This TSF responsible for Platform part of cryptographic operation for PACE, Symmetric Authentication, Terminal Authentication v1 and Active Authentication.
FIA_UAU.5/PACE_EAC1PP	This TSF responsible for Platform part of cryptographic operation for PACE, Chip Authentication Mapping (PACE-CAM), Symmetric Authentication, Terminal Authentication v1.
FIA_UAU.6/PACE_EAC1PP	This TSF responsible for Platform part of cryptographic operation for PACE.
FIA_UAU.6/EAC_EAC1PP	This TSF responsible for Platform part of cryptographic operation for Chip Authentication v1
FIA_API.1/EAC1PP	This TSF responsible the Platform part of cryptographic operation for Chip Authentication v1.
FIA_API.1/PACE_CAM	This TSF responsible the Platform part of cryptographic operation for Chip Authentication Mapping.
FIA_API.1/AA	This TSF responsible the Platform part of cryptographic operation for Active Authentication.
FDP_RIP.1/EAC2PP	This TSF responsible to make unavailable any cryptographic data used in runtime cryptographic computations.
FDP_UCT.1/TRM_EAC2PP	This TSF responsible the Platform part of secure messaging.
FDP_UIT.1/TRM_EAC2PP	This TSF responsible the Platform part of secure messaging.
FDP_RIP.1/EAC1PP	This TSF responsible to make unavailable any cryptographic data used in runtime cryptographic computations.
FDP_UCT.1/TRM_EAC1PP	Equivalent to FDP_UCT.1/TRM_EAC2PP.

FDP_UIT.1/TRM_EAC1PP	Equivalent to FDP_UIT.1/TRM_EAC2PP.
FDP_RIP.1/SSCDPP	This TSF responsible the Platform part of de-allocation of the resource SCD.
FDP_SDI.2/Persistent_SSCDPP	This TSF responsible for integrity of user data.
FDP_SDI.2/DTBS_SSCDPP	This TSF responsible for integrity of user data.
FAU_SAS.1/EAC2PP	This TSF responsible to store the Initialisation and Pre-Personalisation Data in the audit records
FAU_SAS.1/EAC1PP	Equivalent to FAU_SAS.1/EAC2PP.
FMT_SMR.1	This TSF responsible to provide part of the security roles.
FMT_LIM.1/EAC2PP	This TSF responsible to limit its capabilities to enforce the policy as described in the SFR.
FMT_LIM.2/EAC2PP	This TSF responsible to limit its availability to enforce the policy as described in the SFR.
FMT_MTD.1/INI_ENA_EAC2PP	This TSF responsible to restrict the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer.
FMT_MTD.1/INI_DIS_EAC2PP	This TSF responsible to restrict the ability to read out the Initialisation Data and the Pre-personalisation Data to the Personalisation Agent.
FMT_SMF.1/EAC2PP	This TSF responsible to provide part of the security functions.
FMT_SMF.1/EAC1PP	This TSF responsible to provide part of the security functions.
FMT_LIM.1/EAC1PP	Equivalent to FMT_LIM.1/EAC2PP.
FMT_LIM.2/EAC1PP	Equivalent to FMT_LIM.2/EAC2PP.
FMT_MTD.1/INI_ENA_EAC1PP	Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.
FMT_MTD.1/INI_DIS_EAC1PP	Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.
FPT_EMS.1/EAC2PP	This TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timing (measurable at e. g. electrical contacts) that might disclose cryptographic keys.
FPT_FLS.1/EAC2PP	This TSF responsible to preserve a secure state when the failures occur.
FPT_TST.1/EAC2PP	This TSF responsible for the integrity of stored TSF executable code.
FPT_PHP.3/EAC2PP	This TSF ensures resistance to physical attack.
FPT_TST.1/EAC1PP	Equivalent to FPT_TST.1/EAC2PP.
FPT_FLS.1/EAC1PP	Equivalent to FPT_FLS.1/EAC2PP.
FPT_PHP.3/EAC1PP	Equivalent to FPT_PHP.3/EAC2PP
FPT_EMS.1/EAC1PP	This TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timing (measurable at e. g. electrical contacts) that might disclose cryptographic keys.
FPT_EMS.1/SSCDPP	This TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timing (measurable at e. g. electrical contacts) that might disclose cryptographic keys.
FPT_FLS.1/SSCDPP	Equivalent to FPT_FLS.1/EAC2PP.
FPT_PHP.1/SSCDPP	This TSF ensures the passive detection of physical attack.
FPT_PHP.3/SSCDPP	Subsumed by FPT_PHP.3/EAC2PP.
FPT_TST.1/SSCDPP	Subsumed by FPT_TST.1/EAC2PP.
FMT_LIM.1/Loader	This TSF responsible to limit its capabilities to enforce the policy as described in the SFR.

FMT_LIM.2/Loader	This TSF responsible to limit its availability to enforce the policy as described in the SFR.

7.2. Assurance Measures

This section describes the Assurance Measures fulfilling the requirements listed in section 6.2.

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 for functional specification, in the documentation for TOE design, in the security architecture description and in the documentation for implementation representation.
AM_AGD	The guidance documentation is described in the User's Guide documentation [22] and the Administrator's Guide documentation [21].
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 Assurance measures and corresponding documents

7.3. Fulfillment of the SFRs

The following table shows the mapping of the SFRs to security functions of the TOE:

TOE SFR / Security Function	TSF.AccessControl	TSF.Authenticate	TSF.SecureManagement	TSF.CryptoKey	TSF.AppletParametersSign	TSF.Platform
FCS_CKM.1/DH_PACE_EAC2PP	-	-	-	X	-	X
FCS_COP.1/SHA_EAC2PP	-	-	-	X	-	X
FCS_COP.1/SIG_VER_EAC2PP	-	-	-	X	-	X
FCS_COP.1/PACE_ENC_EAC2PP	-	-	-	X	-	X
FCS_COP.1/PACE_MAC_EAC2PP	-	-	-	X	-	X
FCS_CKM.4/EAC2PP	-	-	-	X	-	X
FCS_RND.1/EAC2PP	-	-	-	X	-	X
FCS_CKM.1/DH_PACE_EAC1PP	-	-	-	X	-	X
FCS_CKM.4/EAC1PP	-	-	-	X	-	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	-	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/CA2	-	-	-	X	-	X
FCS_CKM.1/RI	-	-	-	X	-	X
FCS_CKM.1/AA	-	-	-	X	-	X
FCS_COP.1/AA	-	-	-	X	-	X
FCS_CKM.1/CAM	-	-	-	X	-	X
FCS_COP.1/CAM	-	-	-	X	-	X
FCS_CKM.1/SSCDPP	-	-	-	X	-	X
FCS_COP.1/SSCDPP	-	-	-	X	-	X
FIA_AFL.1/Suspend_PIN_EAC2PP	X	X	-	-	-	-
FIA_AFL.1/Block_PIN_EAC2PP	X	X	-	-	-	-
FIA_API.1/CA_EAC2PP	-	X	-	X	-	X
FIA_API.1/RI_EAC2PP	-	X	-	X	-	X
FIA_UID.1/PACE_EAC2PP	X	X	-	-	-	X
FIA_UID.1/EAC2_Terminal_EAC2PP	X	X	-	-	-	X
FIA_UAU.1/PACE_EAC2PP	X	X	-	-	-	X
FIA_UAU.1/EAC2_Terminal_EAC2PP	X	X	-	-	-	X
FIA_UAU.4/PACE_EAC2PP	-	X	-	-	-	X
FIA_UAU.5/PACE_EAC2PP	-	X	-	-	-	X
FIA_UAU.6/CA_EAC2PP	-	X	-	-	-	X
FIA_AFL.1/PACE_EAC2PP	X	X	-	-	-	-

TOE SFR / Security Function	TSF.AccessControl	TSF.Authenticate	TSF.SecureManagement	TSF.CryptoKey	TSF.AppletParametersSign	TSF.Platform
FIA_UAU.6/PACE_EAC2PP	-	X	-	-	-	X
FIA_UID.1/PACE_EAC1PP	X	X	-	-	-	X
FIA_UAU.1/PACE_EAC1PP	X	X	-	-	-	X
FIA_UAU.4/PACE_EAC1PP	-	X	-	-	-	X
FIA_UAU.5/PACE_EAC1PP	-	X	-	-	-	X
FIA_UAU.6/PACE_EAC1PP	-	X	-	-	-	X
FIA_UAU.6/EAC_EAC1PP	-	X	-	-	-	X
FIA_API.1/EAC1PP	-	X	-	X	-	X
FIA_API.1/PACE_CAM	-	X	-	X	-	X
FIA_API.1/AA	-	X	-	X	-	X
FIA_AFL.1/PACE_EAC1PP	X	X	-	-	-	-
FIA_UID.1/SSCDPP	X	-	-	-	-	-
FIA_AFL.1/SSCDPP	X	X	-	-	-	-
FIA_UAU.1/SSCDPP	X	-	-	-	-	-
FDP_ACC.1/TRM_EAC2PP	X	-	-	-	-	-
FDP_ACF.1/TRM	X	X	-	-	-	-
FDP_RIP.1/EAC2PP	-	-	-	X	-	X
FDP_UCT.1/TRM_EAC2PP	-	-	-	X	-	X
FDP_UIT.1/TRM_EAC2PP	-	-	-	X	-	X
FDP_ACC.1/TRM_EAC1PP	X	-	-	-	-	-
FDP_RIP.1/EAC1PP	-	-	-	X	-	X
FDP_UCT.1/TRM_EAC1PP	-	-	-	X	-	X
FDP_UIT.1/TRM_EAC1PP	-	-	-	X	-	X
FDP_ACC.1/SCD/SVD_Generation_SSCDPP	X	-	-	-	-	-
FDP_ACF.1/SCD/SVD_Generation_SSCDPP	X	X	-	-	-	-
FDP_ACC.1/SVD_Transfer_SSCDPP	X	-	-	-	-	-
FDP_ACF.1/SVD_Transfer_SSCDPP	X	X	-	-	-	-
FDP_ACC.1/Signature-creation_SSCDPP	X	-	-	-	-	-
FDP_ACF.1/Signature-creation_SSCDPP	X	X	-	-	-	-
FDP_RIP.1/SSCDPP	-	-	-	X	-	X
FDP_SDI.2/Persistent_SSCDPP	-	-	-	-	-	X
FDP_SDI.2/DTBS_SSCDPP	-	-	-	-	-	X
FTP_ITC.1/PACE_EAC2PP	-	X	-	X	-	-
FTP_ITC.1/CA_EAC2PP	-	X	-	X	-	-
FTP_ITC.1/PACE_EAC1PP	-	X	-	X	-	-
FAU_SAS.1/EAC2PP	-	-	-	-	-	X
FAU_SAS.1/EAC1PP	-	-	-	-	-	X
FMT_MTD.1/CVCA_INI_EAC2PP	X	X	X	-	-	-

TOE SFR / Security Function	TSF.AccessControl	TSF.Authenticate	TSF.SecureManagement	TSF.CryptoKey	TSF.AppletParametersSign	TSF.Platform
FMT_MTD.1/CVCA_UPD_EAC2PP	X	X	X	-	-	-
FMT_SMF.1/EAC2PP	-	-	X	-	-	X
FMT_SMR.1	X	-	-	-	-	X
FMT_MTD.1/DATE_EAC2PP	X	X	X	-	-	-
FMT_MTD.1/PA_EAC2PP	X	X	X	-	-	-
FMT_MTD.1/SK_PICC_EAC2PP	X	X	X	-	-	-
FMT_MTD.1/KEY_READ_EAC2PP	X	-	X	-	-	-
FMT_MTD.1/Initialize_PIN_EAC2PP	-	X	X	-	-	-
FMT_MTD.1/Change_PIN_EAC2PP	-	X	X	-	-	-
FMT_MTD.1/Resume_PIN_EAC2PP	-	X	X	-	-	-
FMT_MTD.1/Unblock_PIN_EAC2PP	-	X	X	-	-	-
FMT_MTD.1/Activate_PIN_EAC2PP	-	X	X	-	-	-
FMT_MTD.3/EAC2PP	-	X	-	-	-	-
FMT_SMR.1/SSCDPP	X	-	-	-	-	-
FMT_SMF.1/SSCDPP	-	X	X	-	-	-
FMT_MOF.1/SSCDPP	X	X	X	-	-	-
FMT_MSA.1/Admin_SSCDPP	X	X	X	-	-	-
FMT_MSA.1/SignatorySSCDPP	X	X	X	-	-	-
FMT_MSA.2/SSCDPP	-	-	X	-	-	-
FMT_MSA.3/SSCDPP	X	X	X	-	-	-
FMT_MSA.4/SSCDPP	-	X	X	-	-	-
FMT_MTD.1/Admin_SSCDPP	X	X	X	-	-	-
FMT_MTD.1/Signatory_SSCDPP	X	X	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	-	-	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	X	X	-	-	-
FMT_MTD.1/CVCA_UPD_EAC1PP	X	X	X	-	-	-
FMT_MTD.1/DATE_EAC1PP	X	X	X	-	-	-
FMT_MTD.1/CAPK_EAC1PP	X	X	X	-	-	-

TOE SFR / Security Function	TSF.AccessControl	TSF.Authenticate	TSF.SecureManagement	TSF.CryptoKey	TSF.AppletParametersSign	TSF.Platform
FMT_MTD.1/PA_EAC1PP	X	X	X	-	-	-
FMT_MTD.1/KEY_READ_EAC1PP	X	-	X	-	-	-
FMT_MTD.3/EAC1PP	-	X	-	-	-	-
FMT_LIM.1/Loader	-	-	-	-	-	X
FMT_LIM.2/Loader	-	-	-	-	-	X
FMT_MTD.1/AA_Private_Key	X	X	X	-	-	-
FPT_EMS.1/EAC2PP	-	-	-	-	-	X
FPT_FLS.1/EAC2PP	-	-	-	-	-	X
FPT_TST.1/EAC2PP	-	-	-	-	X	X
FPT_PHP.3/EAC2PP	-	-	-	-	-	X
FPT_TST.1/EAC1PP	-	-	-	-	X	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	X

7.4.Correspondence of SFR 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.

3882 8. GLOSSARY AND ABBREVIATIONS

3883 For Glossary and Acronyms please refer to the corresponding section of [20].

3884 # 9. Bibliography

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

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

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

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

[5] 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)

[6] 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)

[7] ICAO: Technical Report: Supplemental Access Control for Machine Readable Travel Documents, Version - 1.1, 15. April 2014.

[8] ICAO: ICAO Doc 9303, Part 1: Machine Readable Passports, Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability, Seventh Edition, 2015

[9] ICAO: ICAO Doc 9303 - Machine Readable Travel Documents, 7th edition, 2015

[10] 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)

[11] ISO/IEC 14443 Identification cards — Contactless integrated circuit cards,

[12] ISO/IEC 7816-4:2013 Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange,

[13] BSI: Common Criteria Protection Profile - Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01, v0.01, 22 July 2014

[14] EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation

[15] EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application

[16] BSI: TR-03110-1 - Advanced Security Mechanisms for Machine Readable Travel Documents. Part 1 - eMRTDs with BAC/PACEv2 and EACv1, v2.20 (26. February 2015)

[17] 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) Version 2.21, 21. December 2016

[18] BSI: TR-03110-3 - Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token. Part 3 - Common Specifications v2.21 (21. December 2016)

[19] BSI: TR-03110-4 - Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token. Part 4 – Applications and Document Profiles V2.21, 21. December 2016

[20] BSI: Common Criteria Protection Profile - Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP], BSI-CC-PP-0087 version 1.01, May 20th, 2015

[21] IDentity Applet Suite v3.4 Administrator's Guide v3.4.1 (July 2020)

[22] IDentity Applet Suite v3.4 User's Guide v3.4.5 (October 2022)

[23] JCOP 4 P71 Security Target Lite, Security Target for JCOP 4 P71/SE050 Rev. 4.8 — 8 August 2022

[24] JCOP 4 P71, User manual for JCOP 4 P71, Rev. 4.2, DocNo 469542, 05 August, 2022, NXP Semiconductors

[25] Supporting Document Mandatory Technical Document Composite product evaluation for Smart Cards and similar devices; Version 1.5.1, May 2018

[26] BSI: TR 03111: Elliptic Curve Cryptography, Version 2.0, 28. June 2012.

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

[28] National Institute of Standards and Technology: FIPS PUB 180-4: Secure hash standard, March 2012.

[29] Published by Oracle. Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., May 2015.

[30] European card for e-Services and National e-ID applications, IAS ECC European Citizen Card, Technical Specifications, Revisions 1.0.1.

[31] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie - Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 09. Januar 2013, BSI-TR02102.

[32] Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication, version 1.0, March 8,2016, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan

[33] Protection Profile for ePassport IC with SAC (PACE) and Active Authentication, version 1.0, March 8,2016, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan

[34] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) Security Target Lite, Rev. 2.6, 13 June 2022

[35] Certification Report - NXP Secure Smart Card Controller N7121 with IC NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) BSI-DSZ-CC-1136-V3-2022