Security Target ’CardOS V6.0 ID R1.0’
Rev. 1.91R, Edition 10/2021

Contents

Atos Information Technology GmbH
Otto-Hahn-Ring 6

D-81739 Munich
Germany

Disclaimer of Liability

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcome.

Subject to change without notice.

1 About this Document

1.1 Revision History

Table 1.1: History of released Versions

Version	Release date	Remarks
1.91R	2021-10-21	Release Version

1.2 Acronyms

BAC
Basic Access Control

BIS-BAC
Basic Inspection System - Basic Access Control, see [BSI-CC-PP-0068-V2-2011-MA-01]

CAN
Card Access Number, see [BSI-TR-03110-1-V220], section 2.3.

DTBS
Data To Be Signed

EAC
Extended Access Control

MRTD
Machine Readable Travel Documents

MRZ
Non-block static secret key from Machine-Readable Zone, see [BSI-TR-03110-1-V220], section 2.3.

PACE
Password Authenticated Connection Establishment, see [ICAO-9303-2015], Part 11.

PIN
Personal Identification Number (equivalent to CHV)

PTRNG
Physical True Random Generator (short: physical RNG)

QES
Qualified Electronic Signature

RAD
Reference Authentication Data

SVD
Signature Verification Data

TOE
Target Of Evaluation

VAD
Verification Authentication Data

1.3 Terms and Definitions

Advanced Inspection Procedure

AIP
: A specific order of authentication steps between a travel document and a terminal as required by [ICAO-TR-101], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SO_D and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE.

Common Criteria
: Set of rules and procedures for evaluating the security properties of a product Note 1 to entry: see bibliography for details on the specification of *Common Criteria*.

Evaluation Assurance Level
: Set of assurance requirements for a product, its manufacturing process and its security evaluation specified by *Common Criteria*.

Protection Profile
: Document specifying security requirements for a class of products that conforms in structure and content to rules specified by *Common Criteria*.

Reference Authentication Data
: (RAD) data persistently stored by the TOE for authentication of the signatory.

Security Target
: Document specifying security requirements for a particular product that conforms in structure and content to rules specified by common criteria, which may be based on one or more *Protection Profile*.

Signature Creation Data
: (SCD) unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature (the Directive: 2.4). Note 1 to entry: For the PPs of this standard the SCD is held in the SSCD.

Signature Verification Data
: (SVD) data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature (the Directive: 2.7).

Standard Inspection Procedure

SIP
: A specific order of authentication steps between an travel document and a terminal as required by [ICAO-TR-101], namely (i) PACE or BAC and (ii) Passive Authentication with SOD. SIP can generally be used by BIS-PACE and BIS-BAC.

Target of Evaluation
: Abstract reference in a document, such as a *Protection Profile*, for a particular product that meets specific security requirements.

TOE Security Functions
: Functions implemented by the TOE to meet the requirements specified for it in a *Protection Profile* or *Security Target*.

Verification Authentication Data
: (VAD) data input to an SSCD for authentication of the signatory.

1.4 List of Tables

1.5 List of Figures

2 ST Introduction (ASE_INT)

This section provides document management and overview information that are required by a potential user of the TOE to determine, whether the TOE fulfills her requirements.

For convenience, extensive parts that refer mainly to only one PP are marked as follows:

- PP PACE [BSI-CC-PP-0068-V2-2011-MA-01] is marginalzed with PACE
- PP PACE EAC [BSI-CC-PP-0056-V2-2012-MA-02] is marginalized with EAC
- PP SSCD [BSI-CC-PP-0059-2009-MA-02] is marginalized with SSCD
- PP SSCD KG TCCGA [BSI-CC-PP-0071-2012-MA-01] is marginalized with CGA
- PP SSCD KG TCSCA [BSI-CC-PP-0072-2012-MA-01] is marginalized with SCA

In addition, margins SSCD, PACE or EAC, respectively, are applied, when large text passages concern the SSCD, PACE or EAC functionality.

2.1 ST Reference

Title Security Target 'CardOS V6.0 ID R1.0'

TOE 'CardOS V6.0 ID R1.0'

Sponsor Atos Information Technology GmbH

Editor(s) Atos Information Technology GmbH

CC Version 3.1 (Revision 5)

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

Status Release

Version 1.91R

Date 2021-10-21

Certification ID BSI-DSZ-CC-1162

Keywords ICAO, PACE, EAC, Extended Access Control, ID-Card, Machine Readable Travel Document, CardOS

2.2 TOE Reference

This Security Target refers to the Product 'CardOS V6.0 ID R1.0' (TOE) of Atos Information Technology GmbH for CC evaluation.

2.3 TOE Overview

The Target of Evaluation (*TOE*) ''CardOS V6.0 ID R1.0'' addressed by this Security Target is a smart card with contact-based and contactless interfaces according to TR-03110. The smart card contains at least one application described in the following. In this ST the TOE as a whole is also called card, electronic document or travel document.

Here, an application is a collection of data (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. [BSI-TR-03110-1-V220]),
- all other (common) user data. Other user data are protected by Password Authenticated Connection Establishment (*PACE*, cf. also [BSI-TR-03110-2-V221]). Note that EAC1 recommends prior execution of PACE.

Due to existing migration periods both PACE and Basic Access Control (*BAC*) according to [ICAO-9303-2015] must be supported by MRTD products. However, a terminal or product configuration performing BAC instead of PACE is acting outside of the security policy defined by this ST.

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

Applications considered in [BSI-TR-03110-1-V220] and [BSI-TR-03110-2-V221] are

- an electronic passport (ePass[1]) application,
- an electronic identity (eID) application, and
- a signature (eSign) application.

Atos Information Technology GmbH implemented all these applications in the TOE. Only ePass and eSign application are subject of CC Evaluation.

2.3.1 Usage and major security features of the TOE

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

- only authenticated terminals can get access to the user data stored on the TOE and use security functionality of the card according to the access rights of the terminal,
- the card holder can control access by consciously presenting his card 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 card is averted,
- its security functionality and the data stored inside are self-protected, and
- digital signatures can be created.

For further details, refer to the chapter *Security Requirements (ASE_REQ)* and chapter *TOE Summary Specification (ASE_TSS)*.

[1] The notation of this application is different in the references; both ePass and ePassport are used. In this ST they are used synonymously, too.

2.3.2 TOE Type

The TOE's type addressed by this ST is a smart card with several applications. With the eSign Application the TOE implements a Secure Signature Creation Device according to Regulation (EU) No 910/2014 and the corresponding Implementing Decision [EU-Reg-910-2014]. The ePassport application provides an ICAO-compliant ([ICAO-9303-2015]) ePass Application.

2.3.3 File System of the TOE

The TOE is configured with one of the dedicated file systems during Initialization. Depending on the intended use, the file system of a desired configuration may not contain all applications listed in this ST. Although not all data groups will be present, all mechanisms, such as e.g. access controls and cryptographic operations described in the SFRs of this ST are implemented in these products too. The corresponding security requirements are fulfilled, as soon as the application is available.

The available major Configurations of the file system related to this ST are described in detail in other documents [Atos-V60-ADM]. They do not differ in security-relevant ways. For example, the product configured as *ePassport* provides the same security functionality of an electronic travel document as the product configured as *eID*. Though the latter can be used as a *Qualified Signature Creation Device*, if the eSign application is present, this has no impact on the security functionality of a *ePassport*, not providing this functionality.

The three Major Configurations of the TOE in this Security Target, which differ only in the description of the object system, are:

- *ePassport*: User data are stored in an ICAO-compliant ([ICAO-9303-2015]) ePass Application protected by PACE and EAC1. Here, EAC1 is used only for data groups 3 and 4.
- *SSCD*: User data are stored in [BSI-CC-PP-0059-2009-MA-02] conformant eSign Application.
- *eID*: User data are contained in an ICAO-compliant ([ICAO-9303-2015]) ePass Application, in a [BSI-CC-PP-0059-2009-MA-02] conformant eSign Application, and optional eID applications.

The described technical capabilities of the product as well as the conformance claims of this evaluation aim also at enabling the use of the product as a residence permit using the ePass application.

Observe that the security claims of the security target apply to the ePass and eSign application only. The additional eID applications can be configured in different ways.

The Trust Center acting as the qualified trusted service provider preparing the eSign application can deliver the card in different configurations to the end user. However, in any case the processes in the guidance documentation have to be followed, which ensure that the signature creation functionality of the eSign application is blocked until the legitimate signatory has set the reference authentication data (RAD).

2.3.4 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) with contacts according to [ISO-IEC-7816-part-4] or supporting the contactless communication according to [ISO-IEC-14443-2018].

According to [BSI-TR-03110-2-V221], section 2.1 the TOE is able to recognize the following terminal types:

- *PACE terminal*: A PACE terminal is a basic inspection system. It performs the standard inspection procedure, i.e. PACE followed by Passive Authentication. Afterwards user data are read by the terminal. A PACE terminal is allowed to read only common user data.
- *EAC1 terminal*: An EAC1 terminal is an extended inspection system according to [BSI-TR-03110-1-V220]. It performs the advanced inspection procedure ([BSI-TR-03110-1-V220]) 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.

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 card presenter's restricting input at the terminal. The final CHAT reflects the effective authorization level and is then sent to the TOE [BSI-TR-03110-3-V221]. For the access rights, cf. also the SFR component FDP_ACF.1/TRM.

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 [BSI-TR-03110-3-V221].

The term *terminal* within this ST usually refers to any kind of terminal, if not explicitly mentioned otherwise. Which of the above terminals are related to what application and which data group is accessible by these terminals was given already in chapter *File System of the TOE*.

A terminal shall always start a communication session using PACE. If successfully, it should then proceed with passive authentications. Others than above listed terminals are out of scope of this ST. In particular, terminals using Basic Access Control (BAC) may be functionally supported by the card, but the TOE is not in a certified mode as long as it is operated with BAC (cf. Application note 5 of [BSI-CC-PP-0068-V2-2011-MA-01]).

For communication to the terminal the TOE supports contact-based and contactless communication but requires non-TOE hardware technology (bound-outs, module plates, inlays, antenna technology, etc.) for the physical communication layer.

There is no other explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features.

2.3.5 Conformance to eIDAS

In [EU-Reg-910-2014] the European Parliament and the Council of the European Union has codified the conceptional requirements for qualified electronic signature devices used in the European Union. In the supporting Implementing Decision is stated that an electronic signature device according to eIDAS must be certified using the Common Criteria, claiming conformance to one or more of the protection profiles for Secure Signature Creation Devices. As shown in this ST (see *CC Conformance Claims*) the TOE fulfills these standards and is therefore compliant to signature creation devices according to points (a) of Article 30(3) or 39(2) of the Regulation for qualified electronic signature or seal creation devices.

2.4 TOE Description

According to the Technical Guideline TR-03110 (cf. [BSI-TR-03110-1-V220], section 2.4) the ePass application supports the *Standard Inspection Procedure* and the *Advanced Inspection Procedure*:

Both inspection procedures execute preferably Password Authenticated Connection Establishment (*PACE*) with *CAN* and *MRZ* or alternatively Basic Access Control (*BAC*) as well as Passive Authentication and optionally Active Authentication.

The *Advanced Inspection Procedure* additionally executes Extended Access Control (*EAC*) with Chip Authentication Version 1 and Terminal Authentication Version 1.

Note, that while technically supported *BAC* is not part of this TOE.

The ePass Application can be accessed both through the contact-based and the contactless interface of the TOE according to [BSI-CC-PP-0056-V2-2012-MA-02]. For the eSign Application the interface is not specified in the SSCD PP ([BSI-CC-PP-0059-2009-MA-02]) and both the contact-based or the contactless interface can be used.

For the ePass Application, the card holder can control the access to his user data by conscious presenting his document to authorities[2] (CAN or MRZ authentication as specified in [BSI-TR-03110-1-V220], section 3.3).

For the eSign application, the card holder can control the access to the digital signature functionality by conscious presenting his document to a Service Provider and using his secret Verification Authentication Data for this application: eSign-PIN[3].

Using a secret PIN represents a manifestation of declaration of intent bound to this secret PIN. In order to reflect this fact, the ePass and the eSign Applications shall organizationally get different values of the respective secret PINs (PIN and eSignPIN). It is especially important, since qualified electronic signatures will be generated by the eSign Application. For security reasons this policy will not be enforced by the TOE.

The cryptographic algorithms used by the TOE are configurable. Personalization must be conducted according to the organizational security policies P.Personalization [BSI-CC-PP-0056-V2-2012-MA-02] and P.QSign [BSI-CC-PP-0059-2009-MA-02]. Algorithms and security parameters (e.g. the length of cryptographic keys) of configurations for the certified applications are chosen in accordance to international recommendations [SOG-IS-Crypto-Catalog-V1.2] .

The TOE supports standardized domain parameters defined in the Brainpool standard [RFC-5639-2010-03] and in the NIST standard [NIST-FIPS-186-4] with various key lengths including the corresponding hash functions.

For RSA the TOE also supports various key lengths.

[2] CAN or MRZ user authentication

[3] CAN and eSign-PIN (VAD as specified in [BSI-CC-PP-0059-2009-MA-02], section 3.2.3.5), user authentication, see [BSI-TR-03110-2-V221], section 2.3.

For further details of the supported crypto protocol configurations and parameters refer to section *Elliptic curves used*, *RSA key support*, *Hash functions implemented*, and *Overview of Cryptographic Algorithms*.

PACE and hence the Advanced Inspection Procedure require the use of AES, whereas due to compatibility reasons the Advanced Inspection Procedure with BAC may be used with 3DES (cf. [BSI-TR-03110-3-V221], sections A.2.3.1 and A.2.4.1). Observe that this security target only contains security claims for the inspection procedures involving PACE. The configuration depends on the Initialization of the TOE. A more detailed description is given in the Administrator Guidance [Atos-V60-ADM].

The TOE comprises of

- the circuitry of the chip including all IC Dedicated Software being active in the Operational Phase of the TOE (the integrated circuit, IC),
- the IC Embedded Software (Card Operating System, COS) including configuration and initialization data related to the security functionality of the chip,
- the selected Applications implemented in the file-system to be installed, and
- the associated guidance documentation including description of the file system installation procedure.

The components of the TOE are therefore the hardware (IC) with the operating system CardOS(OS) ready for initialization with a selected dedicated object system. The TOE Design Specification gives a detailed description of the parts of TOE.

The dedicated object systems (file systems) are specified in detail in the Admin Guidance. The file systems support all security functionality and mechanisms described within the ST. After initialization and during personalization, applications (data groups) required for the intended functionality and mechanisms and their access rights are created. Creation of the applications (i.e. the [ISO-IEC-7816-part-4] conforming file structure) including data groups and their access rights) is subject to a limited availability and limited capability policy defined in the family FMT_LIM. In particular, the TOE initialization mechanisms ensure that creation or alteration of the file system is not possible after the manufacturing phase (this excludes populating data groups with values, as is done in the personalization phase). This is necessary for the manufacturer to use a single IC for different configurations.

The Guidance documentation ([Atos-V60-ADM]) provides further requirements for the manufacturer and security measures required for protection of the TOE until reception by the end-user.

The hardware platform of the TOE is identified as SLC52GDA448* (CC certification identifier IFX_CCI_000005 Design Step H13), which means that this ST applies to all derivates of the IFC_CCI_000005. For the TOE the following derivates will be used which differ only in the input capacities on the contactless interface:

- SLC52GDA448A8, 27pF
- SLC52GDA448A9, 78pF

The chips can be delivered as wafer, or packaged in the modules M8.8, MCC8, MCS8 (27pF) or COM10.6, COM 10.8 (78pF) or other modules or packages. In case of a contactless module, the module may be integrated in an antenna inlay, which is then used to build a optically and machine readable smart card or ePassport booklet. A dual interface module may be integrated in a smart card. Note that the different contact technologies are not considered part of the TOE.

Since CardOS is implemented on an already certified IC (certification number BSI-DSZ-CC-1110-V3-2020) the evaluation considers the composite evaluation aspects ([BSI-AIS36-V5]). This composite ST is based on the ST of the underlying platform ([Infineon-ST-SLC52-H13]), which claims conformance to Security IC Platform Protection Profile ([BSI-CC-PP-0084-2014]). The compatibility between this ST and the platform ST is considered in detail in section *Compatibility between the Composite ST and the Platform-ST*.

2.4.1 Life Cycle Phases Mapping

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 completion of the operating system, installation of the smart card applications and their electronic personalization, i.e. tying the application data up to the card holder.

Operational use of the TOE is explicitly in the focus of the Protection Profiles. Nevertheless, some TOE functionality is already available in the manufacturing and the card issuing life cycle phases. Therefore it is also considered by the Protection Profiles and this ST.

In compliance to the Protection Profiles, the TOE life cycle is described in terms of the following four life cycle phases, divided in steps.

Life cycle phase A "Development"

Step 1: The TOE is developed in phase 1. The IC developer develops

- the integrated circuit,
- the IC dedicated software and
- the guidance documentation associated with these TOE components.

Step 2: The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC dedicated software, and develops the IC embedded software (operating system), the card application(s) and the guidance documentation associated with these TOE components.

The software developer ships the IC embedded software in accordance with the certified delivery and loading procedures to the IC manufacturer. Furthermore, the software developer ships load scripts which in particular contain the certified object system layout(s) for the various configurations as well as the relevant guidance documentation securely to the Initializer.

Life cycle phase B "IC Manufacturing"

Step 3: In a first step, the TOE integrated circuit is produced. The IC manufacturer writes IC identification data onto the chip in order to track and control the IC as dedicated card material during IC manufacturing, and during delivery to the electronic document manufacturer. Additionally, the IC manufacturer adds the IC embedded software in the non-volatile programmable memory using the certified loading mechanisms of the IC.

The IC is securely delivered from the IC manufacturer to the composite product manufacturer.

The IC may be delivered as a wafer, module or a packaged component.

Life cycle phase C "Composite Product Integration and Initialization"

Step 4 (optional): The composite product manufacturer

- produces modules, or packaged components, combined with hardware for the contact-based or contactless interfaces (e.g. inlays)

Step 5: The initializer

- equips the card's chip with pre-personalization data, and
- creates the application(s).

The creation of the application(s) is conducted by the *Initialization* of the card using secured load scripts to create the object system(s) for the certified ePass and/or eSign application(s) on the card. The *Initialization* also optionally includes the creation of the SCD/SVD pair for the signatory in the eSign application (cf. Application note 1 of [BSI-CC-PP-0068-V2-2011-MA-01] and [BSI-CC-PP-0056-V2-2012-MA-02]).

Observe that additional eID applications can be loaded in this step as well.

The *Initialization* can also be organizationally and or physically separated from the other card manufacturing steps.

After the *Initialization* the card is ready for import of user data (Personalization).

The pre-personalized TOE together with the IC identifier is securely delivered from the *Initializer* to the *Personalization*. The *Initializer* also provides the relevant parts of the guidance documentation. The Administrator Personalization Key is also delivered securely to the *Personalization*.

Life cycle phase D "Personalization"

Step 6: The *Personalization* of the card includes for the ePass application:

1) the survey of the card holder's biographical data,
2) the enrollment of the card 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 card, and
4) configuration of the TSF, if necessary.

and for the eSign application:

1) optional creation of the SCD/SVD pair for the signatory
2) export of the SVD to for creation and subsequent storage of the card holder certificate

Parts of the configuration of the TSF is performed during *Personalization* 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 card holder for operational use.

The TSF data (data created by and for the TOE, that affects the operation of the TOE; cf. [CC-Part1-V3.1] § 92) comprise (but are not limited to) the Personalization Agent Authentication Key(s), the Terminal Authentication trust anchor, the effective date and the Chip Authentication Private Key. (cf. Application note 2 of [BSI-CC-PP-0068-V2-2011-MA-01] and [BSI-CC-PP-0056-V2-2012-MA-02]).

This ST distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [ICAO-9303-2015]. This approach allows but does not enforce the separation of these roles. (cf. Application note 3 of [BSI-CC-PP-0068-V2-2011-MA-01] and [BSI-CC-PP-0056-V2-2012-MA-02])

From a hardware point of view, this cycle phase is already an operational use of the composite product and not a personalization of the hardware. The hardware's "Personalization" (cf. [Infineon-ST-SLC52-H13]) ends with the *Installation* of the TOE (installation of the object system).

The Personalization with User Data, e.g. card holder identification data, may be separated from the personalization of the TOE as Qualified Signature Creation Device, e.g. the generation of a signature key.

The Personalization as a personalized SSCD includes the SVD certification for the intended user according to [EU-Reg-910-2014] and the delivery to the legitimate user.

Life cycle phase E "Operational Use"

Step 7: The chip of the TOE is used by the card 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.

This ST considers at least the phases A and B (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase. (cf. Application note 4 of [BSI-CC-PP-0068-V2-2011-MA-01] and [BSI-CC-PP-0056-V2-2012-MA-02]).

Correspondence to the Life-Cycle Description in the Protection Profile

Following the [BSI-CC-PP-0084-2014] Protection Profile, section 1.2.3 the life cycle phases of a smart card can be divided into the following seven phases:

Phase 1: IC Embedded Software Development

Phase 2: IC Development

Phase 3: IC Manufacturing

Phase 4: IC Packaging

Phase 5: Composite Product Integration

Phase 6: Personalization

Phase 7: Operational Use

Phase A “Development”, step 1 and step 2 cover exactly phase 1 and phase 2 of [BSI-CC-PP-0084-2014].

Phase B “IC Manufacturing” covers phase 3 of [BSI-CC-PP-0084-2014] completely and is conducted based on the certified production procedures of the IC.

The TOE can be delivered in various form factors. Thus, IC packaging i.e. phase 4 of [BSI-CC-PP-0084-2014] is conducted either in the IC Manufacturing already (phase B) or at a later stage during the composite product integration (phase C). Phase C also covers phase 5 of [BSI-CC-PP-0084-2014] completely.

Phase D “Personalization” directly corresponds to phase 6 of [BSI-CC-PP-0084-2014].

Observe, that the TOE has reached its secure state already at the delivery point which is between phase B to phase C. Up to this point, the secure handling is controlled by the guidelines and security mechanisms provided by the IC manufacturer. After this point, the secure handling during *Initialization* and *Personalization* is controlled by the guidelines and security mechanisms provided by the TOE developer. In particular, observe that both the *Initialization* and the *Personalization* must be conducted in a trusted environment (c.f. OE.Env_Admin).

The security environment for the TOE and the ST of the underlying platform match, the IC life cycle phases up to 6 are covered by a controlled environment as required in [Infineon-ST-SLC52-H13], section 7.3.1.2. In IC life cycle phase 7 no restrictions apply.

The last life cycle phase E corresponds to the first step of Phase 7 of [BSI-CC-PP-0084-2014].

2.4.2 TOE Boundaries

2.4.2.1 TOE Physical Boundaries

Smart card as used in this ST means an integrated circuit containing a microprocessor, (CPU), a coprocessor for special (cryptographic) operations, a random number generator, volatile and non-volatile memory, and associated software, packaged and embedded in a carrier. The integrated circuit is a single chip incorporating CPU and memory, which include RAM, ROM, and non-volatile memory.

The chip is embedded in a module, which provides the capability for standardized connection to systems separate from the chip through TOE’s interfaces in accordance with ISO standards.

The physical constituent of the TOE is IC with the operating system loaded using the certified loading processes of the IC manufacturer and a set of load scripts which allow for installing the object system in a dedicated configuration.

The IC can be physically delivered on wafers, or as modules, or inlays but the physical boundary of the TOE is the IC itself excluding the connection technology.

After the *Installation* of the object system, the TOE can be personalized for the end-usage phase for the document holder as a card.

2.4.2.2 TOE Logical Boundaries

All card accepting devices (Host Applications) will communicate through the I/O interface of the operating system by sending and receiving octet strings. The logical boundaries of the TOE are given by the complete set of commands of the CardOS operating system for access, reading, writing, updating or erasing data.

The input to the TOE is transmitted over the physical interface as an octet string that has the structure of Command Application Protocol Data Unit (CAPDU). The output octet string from the TOE has the structure of a Response Application Protocol Data Unit (RAPDU).

The Application Protocol Data Units or CardOS commands that can be used in the operating systems are described in more detail in the guidance [Atos-V60-ADM], [Atos-V60-USR].

2.4.2.3 TOE Delivery Format

In summary the delivery of the TOE consists of:

- the integrated circuit (IC) with the operation system pre-loaded
- the administrator and user guidance documentation [Atos-V60-ADM], [Atos-V60-USR]
- personalization information package, required for the secure personalization of the TOE. Further details about the secure personalization are provided in the guidance documentation.

3 Conformance Claim

3.1 CC Conformance Claims

This Security Target claims conformance to Common Criteria for Information Technology Security Evaluation [CC],

Part 1: Introduction and general model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017, [CC-Part1-V3.1]

Part 2: Security functional components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017, [CC-Part2-V3.1]

Part 3: Security assurance components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017, [CC-Part3-V3.1]

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, [CEM-V3.1] has to be taken into account.

3.2 PP Claims

This ST claims *strict* conformance to

- Common Criteria Protection Profile 'Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP)', [BSI-CC-PP-0056-V2-2012-MA-02]

Since this PP claims strict conformance to [BSI-CC-PP-0068-V2-2011-MA-01], this ST implicitly also claims *strict* conformance to

- Common Criteria Protection Profile 'Machine Readable Travel Document using Standard Inspection Procedure with PACE', [BSI-CC-PP-0068-V2-2011-MA-01].

However, since [BSI-CC-PP-0056-V2-2012-MA-02] already claims strict conformance to [BSI-CC-PP-0068-V2-2011-MA-01], and basically extends this PP by the use of PACE within the EAC protocol this implicit conformance claim is not always made explicit for the sake of presentation. Nonetheless, if necessary to yield a better overview, references to this Protection Profile are given or the relation with this PP is explained.

This ST claims also strict conformance to

- Common Criteria Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation, EN 419211-2:2013, [BSI-CC-PP-0059-2009-MA-02]
- Common Criteria Protection Profiles for Secure Signature Creation Device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, EN 419211-4:2013, [BSI-CC-PP-0071-2012-MA-01]
- Common Criteria Protection Profiles for Secure Signature Creation Device – Part 5: Extension for device with key generation and trusted communication with signature creation application, EN 419211-5:2013, [BSI-CC-PP-0072-2012-MA-01]

Application Note 6: The conformance claim to the Secure Signature Creation Device protection profiles covers the part of the security policy for the eSign application of the TOE, and hence are applicable, if the eSign application is operational.

3.3 Package Claims

The evaluation of the TOE is a composite evaluation and uses the results of the CC evaluation provided by [Infineon-ST-SLC52-H13]. The IC hardware platform and its primary embedded software are evaluated at level EAL 6+.

The evaluation assurance level of the TOE is EAL4 as defined in [CC-Part3-V3.1] augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

3.4 Conformance Claim Rationale

The TOE type is a chip consistent with the TOE type of the claimed PPs [BSI-CC-PP-0056-V2-2012-MA-02] and [BSI-CC-PP-0059-2009-MA-02], [BSI-CC-PP-0071-2012-MA-01], and [BSI-CC-PP-0072-2012-MA-01]. 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 TR-03110, and additionally representing for the eSign application a combination of hardware and software configured to securely create, use and manage signature-creation data.
2. The implementation standards have developed further since the last publication of the PACE/EAC Protection Profiles. However, the standards contain primarily extensions that are not related to the PACE and EAC protocol steps. The only exception is the introduction of the PACE-Chip Authentication Mapping but this is just a combination of the existing mechanisms for optimization purposes. Therefore, this ST assumes that the protection profile can still be used "mutatis mutandis" also with newer versions of the implementation standards. Some clarifications have been added to the various elements of the security problem definitions, security objectives and the security functional requirements but all of these do not change the original definitions.
3. 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. Two assumptions have been added to the ST:
   - A.Env_Admin and A.Env_Mass_Signature capture assumptions on the specific use of TOE functions in the Initialization and Personalization as well as using the TOE for mass signature generation. These assumptions do not contradict the original security problem definition.
4. The security objectives for the TOE in this ST include all the security objectives for the TOE of the claimed PPs. One additional security objective is added to the ST:
   - OT.AA_Proof models the additional objective of the TOE to provide the Active Authentication feature. There are no corresponding additions to the SPD because Active Authentication is just another mean (in addition to the Chip Authentication modelled in the PP) to counter the threat T.Counterfeit. Therefore, this extension does not contradict the protection profiles this ST claims conformance to.
5. The security objectives for the operational environment in this ST include all security objectives for the operational environment of the claimed PPs. The following objectives for the environment have been added or refined in this ST:
   - OE.Env_Admin and OE.Env_Mass_Signature capture the additional assumptions A.Env_Admin and A.Env_Mass_Signature and therefore, don't contradict the protection profiles.
   - OE.AA_Key_Travel_Document has been added and OE.Exam_Travel_Document has been refined to mandate that the Inspection system uses Active Authentication (c.f. OT.AA_Proof) when supported in the configuration and Chip Authentication is

not used. This extension obviously does not contradict to the objectives definitions in the PPs.

6. The SFRs specified in this ST include all security functional requirements (SFRs) specified in the claimed PPs. There are several refined or added SFRs within this ST:
   - The SFR FIA_UAU.1/SSCDPP is redefined from [BSI-CC-PP-0059-2009-MA-02] by additional assignments, this does not violate strict conformance to [BSI-CC-PP-0059-2009-MA-02].
   - 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 and EAC1 protected user data. These access control SFPs and security roles are unified to FDP_ACF.1/TRM and FMT_SMR.1
   - The SFRs FIA_API.1/AA, FMT_MTD.1/CA_AA_PK, FCS_COP.1/AA_SGEN_EC, and FCS_COP.1/AA_SGEN_RSA are added to model the additional Active Authentication feature for the ePass application. Since this feature does not interfere with the other security features this extension does not contradict to the definitions in the protection profiles
   - The SFR FIA_UAU.6/Signature_Creation was added to model the specific behavior of the TOE when generating mass signatures. This extensions does not contradict the definitions in the protection profiles because the TOE offers this functionality under control of the signatory.
   - The SFRs FIA_AFL.1/Suspend_PIN and FIA_AFL.1/Block_PIN have been added to explicitly include the suspend and blocking mechanisms for PACE-PINs. Since these SFRs have been directly taken over from the PP [BSI-CC-PP-0086-2015] which updates the PPs that this ST claims conformance to including newer protocol variants, the addition does not contradict the conformance claims.
7. The SARs specified in this ST are the same as specified in the claimed PPs or extend them.

The TOE type definitions of the claimed PPs ([BSI-CC-PP-0056-V2-2012-MA-02], [BSI-CC-PP-0059-2009-MA-02]) differ slightly, however the TOE type definitions are not inconsistent. To avoid renaming in this ST all the notations of the different PPs are taken over here.

4 Security Problem Definition

4.1 Assets and External Entities

Primary Assets

user data stored on the TOE All data (being not authentication data) stored in the context of the ePassport application of the travel document as defined in [ICAO-TR-110] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-TR-110]). This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [BSI-CC-PP-0055-110]. *PACE EAC*

user data transferred between the TOE and the terminal connected All data (being not authentication data) being transferred in the context of the ePassport application of the travel document as defined in [ICAO-TR-110] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-TR-110]). User data can be received and sent (exchange <=> {receive, send}). *PACE EAC*

travel document tracing data Technical information about the current and previous locations of the travel document gathered unnoticeable by the travel document holder recognising the TOE not knowing any PACE password. TOE tracing data can be provided / gathered. *PACE EAC*

Logical travel document sensitive User Data Sensitive biometric reference data (EF.DG3, EF.DG4) *EAC*

Due to interoperability reasons the ICAO standard [ICAO-TR-110] requires that Basic Inspection Systems may have access to logical travel document data DG1, DG2, DG5 to DG16. The TOE is not in certified mode, if it is accessed using BAC. Note that the BAC mechanism cannot resist attacks with high attack potential. If supported, it is therefore recommended to used PACE instead of BAC. If nevertheless BAC has to be used, it is recommended to perform Chip Authentication v.1 before getting access to data (except DG14), as this mechanism is resistant to high potential attacks.

Authenticity of the travel document's chip The authenticity of the travel document's chip personalised by the issuing State or Organisation for the travel document holder is used by the traveller to prove his possession of a genuine travel document. *EAC*

SCD private key used to perform an electronic signature operation.

The confidentiality, integrity and signatory's sole control over the use of the SCD shall be maintained. *SSCD CGA SCA*

SVD public key linked to the SCD and used to perform electronic signature verification.

The integrity of the SVD when it is exported shall be maintained. *SSCD CGA SCA*

DTBS, DTBS/R set of data, or its representation, which the signatory intends to sign.

Their integrity and the unforgeability of the link to the signatory provided by the electronic signature shall be maintained. *SSCD CGA SCA*

In order to achieve a sufficient protection of the primary assets listed above, the following secondary assets are also protected by the TOE. The secondary assets represent TSF and TSF data in the sense of CC.

Secondary Assets

Accessibility to the TOE functions and data only for authorised subjects Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only. *PACE*

Genuineness of the TOE Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. This asset also covers 'Authenticity of the MRTD's chip' in [BSI-CC-PP-0055-110]. ***PACE***

TOE internal secret cryptographic keys Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality. ***PACE***

TOE internal non-secret cryptographic material Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SO_D containing digital signature) used by the TOE in order to enforce its security functionality. ***PACE***

travel document communication establishment authorisation data Restricted-revealable[1] authorisation information for a human user being used for verification of the authorisation attempts as authorised user (PACE password). These data are stored in the TOE and are not to be send to it. ***PACE***

Since the travel document does not support any secret travel document holder authentication data and the latter may reveal, if necessary, his or her verification values of the PACE password to an authorised person or device, a successful PACE authentication of a terminal does not unambiguously mean that the travel document holder is using TOE (cf. Application note 7 of [BSI-CC-PP-0068-V2-2011-MA-01]).

travel document communication establishment authorisation data are represented by two different entities: (i) reference information being persistently stored in the TOE and (ii) verification information being provided as input for the TOE by a human user as an authorisation attempt. The TOE shall secure the reference information as well as – together with the terminal connected[2] – the verification information in the 'TOE <-> terminal' channel, if it has to be transferred to the TOE. Please note that PACE passwords are not to be send to the TOE (cf. Application note 8 of [BSI-CC-PP-0068-V2-2011-MA-01]).

Subjects and external entities

travel document holder A person for whom the travel document Issuer has personalised the travel document[3]. This entity is commensurate with 'MRTD Holder' in [BSI-CC-PP-0055-110]. ***PACE EAC***

Please note that a travel document holder can also be an attacker (s. below).

travel document presenter

traveller A person presenting the travel document to a terminal[4] and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveller' in [BSI-CC-PP-0055-110]. ***PACE EAC***

Please note that a travel document presenter can also be an attacker (s. below).

Terminal A terminal is any technical system communicating with the TOE through the contactless/contact interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as not being PACE authenticated ('Terminal' is used by the travel document presenter). This entity is commensurate with 'Terminal' in [BSI-CC-PP-0055-110]. ***PACE EAC***

Basic Inspection System with PACE

BIS-PACE A technical system being used by an inspecting authority[5] and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric ***PACE EAC***

[1] The travel document holder may reveal, if necessary, his or her verification values of CAN and MRZ to an authorised person or device who definitely act according to respective regulations and are trustworthy.
[2] the input device of the terminal
[3] i.e. this person is uniquely associated with a concrete electronic Passport
[4] in the sense of [ICAO-TR-110]
[5] concretely, by a control officer

data (DG2) of the travel document holder). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication.

Document Signer

DS An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [ICAO-9303-2015]. This role is usually delegated to a Personalisation Agent. ***PACE EAC***

Country Signing Certification Authority

CSCA An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel document and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (C_{CSCA}) having to be distributed acc. to [ICAO-9303-2015], Part 12, 5 ***PACE EAC***

Personalisation Agent An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: ***PACE EAC***

(i) establishing the identity of the travel document holder for the biographic data in the travel document,

(ii) enrolling the biometric reference data of the travel document holder,

(iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [ICAO-9303-2015],

(iv) writing the document details data,

(v) writing the initial TSF data,

(vi) signing the Document Security Object defined in [ICAO-9303-2015] (in the role of DS).

Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. This entity is commensurate with 'Personalisation agent' in [BSI-CC-PP-0055-110].

Manufacturer Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer. This entity is commensurate with 'Manufacturer' in [BSI-CC-PP-0055-110]. ***PACE EAC***

Attacker A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most high attack potential. Please note that the attacker might 'capture' any subject role recognised by the TOE. This external entity is commensurate with 'Attacker' in [BSI-CC-PP-0055-110]. ***PACE***

EAC

A threat agent trying

(i) to manipulate the logical travel document without authorization,

(ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4),

(iii) to forge a genuine travel document, or

(iv) to trace a travel document.

Human or process acting on their behalf located outside the TOE. The main goal of the attacker is to access the SCD or to falsify the electronic signature. The attacker has got a high attack potential and knows no secret.

SSCD CGA SCA

Country Verifying Certification Authority

CVCA The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organisation with respect to the protection of sensitive biometric reference data stored in the travel document. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link- Certificates.

EAC

DV

Document Verifier The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the travel document in the limits provided by the issuing States or Organisations in the form of the Document Verifier Certificates.

EAC

Inspection system

IS A technical system used by the border control officer of the receiving State

EAC

(i) examining an travel document presented by the traveller and verifying its authenticity and

(ii) verifying the traveller as travel document holder.

Extended Inspection System

EIS The Extended Inspection System (EIS) performs the Advanced Inspection Procedure and therefore

EAC

(i) contains a terminal for the communication with the travel document's chip,

(ii) implements the terminals part of PACE and/or BAC;

(iii) gets the authorization to read the logical travel document either under PACE or BAC by optical reading the travel document providing this information.

(iv) implements the Terminal Authentication and Chip Authentication Protocols both Version 1 according to [BSI-TR-03110-1-V220] and

(v) is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the *BIS-PACE*, PACE must be used.

User End user of the TOE who can be identified as administrator or signatory.

The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.

SSCD CGA SCA

Administrator User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions.

The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.

SSCD CGA SCA

Signatory User who hold the TOE and use it on their own behalf or on behalf of the natural or legal person or entity they represent.

SSCD CGA SCA

The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.

4.2 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 TOE's use in the operational environment.

4.2.1 T.Skimming (Skimming travel document / Capturing Card-Terminal Communication)

PACE EAC

Adverse action An attacker imitates an inspection system in order to get access to the *user data stored on* or *transferred between the TOE and the inspecting authority connected* via the contactless/contact interface of the TOE.

Threat agent having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset confidentiality of logical travel document data

Notes

1. This TOE does not support *BAC*.
2. A product using *BIS-BAC* cannot avert this threat in the context of the security policy defined in this ST. (cf. application note 10 of [BSI-CC-PP-0068-V2-2011-MA-01]).
3. MRZ is printed and CAN is printed or stuck on the travel document. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. *OE.Travel_Document_Holder (Travel document holder Obligations)*. (cf. application note 11 of [BSI-CC-PP-0068-V2-2011-MA-01]).

4.2.2 T.Eavesdropping (Eavesdropping on the communication between the TOE and the PACE terminal)

PACE EAC

Adverse action An attacker is listening to the communication between the travel document and the PACE authenticated *BIS-PACE* in order to gain the *user data transferred between the TOE and the terminal connected*.

Threat agent having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset confidentiality of logical travel document data

Notes

1. This TOE does not support *BAC*.
2. A product using *BIS-BAC* cannot avert this threat in the context of the security policy defined in this ST. (cf. application note 10 of [BSI-CC-PP-0068-V2-2011-MA-01]).

4.2.3 T.Tracing (Tracing travel document)

PACE EAC

Adverse action An attacker tries to gather *TOE tracing data* (i.e. to trace the movement of the travel document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless/contact interface of the TOE.

Threat agent having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset privacy of the travel document holder

Notes

1. This threat completely covers and extends "T.Chip-ID" from BAC PP [BSI-CC-PP-0055-110], (cf. application note 13 of [BSI-CC-PP-0068-V2-2011-MA-01]).
2. A product using *BAC* (whatever the type of the inspection system is: *BIS-BAC*) cannot avert this threat in the context of the security policy defined in this ST. (cf. application note 14 of [BSI-CC-PP-0068-V2-2011-MA-01]).

4.2.4 T.Forgery (Forgery of Data)

PACE EAC

Adverse action An attacker fraudulently alters the *User Data* or/and *TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected* in order to outsmart

(i) the PACE authenticated *BIS-PACE* or

(ii) the authenticated Extended Inspection System[6] *EAC*

by means of changed travel document holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.

Threat agent having high attack potential

Asset integrity of the travel document

4.2.5 T.Abuse-Func (Abuse of Functionality)

PACE EAC

Adverse action An attacker may use functions of the TOE which shall not be used in TOE operational phase in order

(i) to manipulate or to disclose the *User Data stored in the TOE*,

(ii) to manipulate or to disclose the *TSF-data stored in the TOE* or

(iii) to manipulate (bypass, deactivate or modify) *soft-coded security functionality of the TOE*.

This threat addresses the misuse of the functions for the initialisation and personalisation in the operational phase after delivery to the travel document holder.

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

Asset integrity and authenticity of the travel document, availability of the functionality of the travel document

[6] T.Forgery is extended by (ii) due to PP [BSI-CC-PP-0056-V2-2012-MA-02] Application note 8.

Notes

1. Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here (cf. application note 16 of [BSI-CC-PP-0068-V2-2011-MA-01]).

4.2.6 T.Information_Leakage (Information Leakage from travel document)

PACE *EAC*

Adverse action An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.

Threat agent having high attack potential

Asset confidentiality of User Data and TSF-data of the travel document

4.2.7 T.Phys-Tamper (Physical Tampering)

PACE *EAC*

Adverse action An attacker may perform physical probing of the travel document in order

(i) to disclose the TSF-data, or

(ii) to disclose/reconstruct the TOE's Embedded Software.

An attacker may physically modify the travel document in order to alter (i) its security functionality (hardware and software part, as well), (#) the User Data or the TSF-data stored on the travel document.

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

Asset integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document

Notes

1. Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g. authentication key of the travel document) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires a direct interaction with the travel document's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary. (cf. application note 18 of [BSI-CC-PP-0068-V2-2011-MA-01]).

4.2.8 T.Malfunction (Malfunction due to Environmental Stress)

PACE
EAC

Adverse action An attacker may cause a malfunction the travel document's hardware and Embedded Software by applying environmental stress in order to

(i) deactivate or modify security features or functionality of the TOE' hardware or to

(ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software.

This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting errors in the travel document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent having high attack potential, being in possession of one or more legitimate travel documents, having information about the functional operation

Asset integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document

---

Notes

1. A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the threat T.Phys-Tamper) assuming a detailed knowledge about TOE's internals. (cf. application note 19 of [BSI-CC-PP-0068-V2-2011-MA-01]).

4.2.9 T.Read_Sensitive_Data (Read the sensitive biometric reference data)

EAC

Adverse action An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel document's chip. The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [BSI-CC-PP-0055-110]) in respect of the attack path (communication interface) and the motivation (to get data stored on the travel document's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods.

Note, that the sensitive biometric reference data are stored only on the travel document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the travel document as well.

Threat agent having high attack potential, knowing the PACE Password, being in possession of a legitimate travel document

Asset confidentiality of logical travel document sensitive user data (i.e. biometric reference)

4.2.10 T.Counterfeit (Counterfeit of travel document chip data)

EAC

Adverse action An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine travel document's chip to be used as part of a counterfeit travel document. This violates the authenticity of the travel document's chip used for authentication of a traveller by possession of a travel document. The attacker may generate a new data set or extract completely or partially the data from a genuine travel document's chip and copy them to another appropriate chip to imitate this genuine travel document's chip.

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

Asset authenticity of user data stored on the TOE

4.2.11 T.SCD_Divulg (Storing, copying and releasing of the signature creation data)

SSCD
CGA
SCA

Adverse action An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage and use for signature creation in the TOE.

4.2.12 T.SCD_Derive (Derive the signature creation data)

SSCD
CGA
SCA

Adverse action An attacker derives the SCD from publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data exported outside the TOE, which is a threat against the secrecy of the SCD.

4.2.13 T.Hack_Phys (Physical attacks through the TOE interfaces)

SSCD
CGA
SCA

Adverse action An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

Notes

PACE

1. This threat is also directed against the PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}), the ephemeral private key ephem-SK_{PICC}-PACE, Chip Authentication private key, Administrator Personalization Key and Chip Authentication session keys (CA-K_{MAC}, CA-K_{Enc}).

4.2.14 T.SVD_Forgery (Forgery of the signature verification data)

SSCD
CGA
SCA

Adverse action An attacker forges the SVD presented by the CSP to the CGA. This results in loss of SVD integrity in the certificate of the signatory.

4.2.15 T.SigF_Misuse (Misuse of the signature creation function of the TOE)

SSCD CGA SCA

Adverse action An attacker misuses the signature creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

4.2.16 T.DTBS_Forgery (Forgery of the DTBS/R)

SSCD CGA SCA

Adverse action An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS the signatory intended to sign.

4.2.17 T.Sig_Forgery (Forgery of the electronic signature)

SSCD CGA SCA

Adverse action An attacker forges a signed data object, maybe using an electronic signature that has been created by the TOE, and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature created by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

4.3 Organizational Security Policies

The TOE and/or its environment shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see [CC-Part1-V3.1], sec. A.6.3). This ST includes the OSPs from the claimed protection profiles as listed below and provides no further OSPs.

4.3.1 P.Manufact (Manufacturing of the travel document's chip)

PACE EAC

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The travel document Manufacturer writes the Pre-personalisation Data which contains at least the Personalisation Agent Key.

Notes

1. OSP P.Manufact covers OSP "P.Process-TOE" of [Infineon-ST-SLC52-H13] which inherits OSP "P.Process-TOE" from PP [BSI-CC-PP-0084-2014].

4.3.2 P.Pre-Operational (Pre-operational handling of the travel document)

PACE ***EAC***

1) The travel document Issuer issues the travel document and approves it using the terminals complying with all applicable laws and regulations.
2) The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE[7].
3) The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase, cf. sec. 1.2.3 in [BSI-CC-PP-0068-V2-2011-MA-01].
4) If the travel document Issuer authorises a Personalisation Agent to personalise the travel document for travel document holders, the travel document Issuer has to ensure that the Personalisation Agent acts in accordance with the travel document Issuer's policy.

4.3.3 P.Card_PKI (PKI for Passive Authentication (issuing branch))

Note

The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

PACE ***EAC***

1) The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (*CSCA*). The travel document Issuer shall publish the CSCA Certificate (C_{CSCA}) .
2) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (C_{CSCA}) having to be made available to the travel document Issuer by strictly secure means, [ICAO-9303-2015]. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the travel document Issuer, see [ICAO-9303-2015].
3) A Document Signer shall
   (i) generate the Document Signer Key Pair,
   (ii) hand over the Document Signer Public Key to the CSCA for certification,
   (iii) keep the Document Signer Private Key secret and
   (iv) securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.

[7] cf. Table 1 and Table 2 in [BSI-CC-PP-0068-V2-2011-MA-01]

4.3.4 P.Trustworthy_PKI (Trustworthiness of PKI)

PACE EAC

The CSCA shall ensure that it issues its certificates exclusively to the rightful organisations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the travel document.

4.3.5 P.Terminal (Abilities and trustworthiness of terminals)

PACE EAC

The Basic Inspection Systems with PACE (*BIS-PACE*) shall operate their terminals as follows:

1) The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders as defined in [ICAO-9303-2015].

2) They shall implement the terminal parts of the PACE protocol [ICAO-TR-110], of the Passive Authentication [ICAO-9303-2015] and use them in this order[8]. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

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 o fC_{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, [ICAO-9303-2015]).

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 current PP.

Notes

1. P.Terminal holds also for Extended Inspection System with PACE.

4.3.6 P.Sensitive_Data (Privacy of sensitive biometric reference data)

EAC

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the travel document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organisation authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The travel document's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication Version 1 **or PACE Chip Authentication Mapping, respectively**[9].

[8] This order is commensurate with [ICAO-TR-110].
[9] since Chip Authentication functionally is part of PACE Chip Authentication Mapping

4.3.7 P.Personalisation (Personalisation of the travel document by issuing State or Organisation only)

EAC

The issuing State or Organisation guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical travel document with respect to the travel document holder.

The personalisation of the travel document for the holder is performed by an agent authorized by the issuing State or Organisation only.

4.3.8 P.CSP_QCert (Qualified certificate)

SSCD CGA SCA

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. the directive, Article 2, Clause 9, and Annex I) for the SVD generated by the SSCD. The certificates contain at least the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

4.3.9 P.QSign (Qualified electronic signatures)

SSCD CGA SCA

The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. the directive, Article 1, Clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to the directive Annex I)[10]. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

4.3.10 P.Sigy_SSCD (TOE as secure signature creation device)

SSCD CGA SCA

The TOE meets the requirements for an SSCD laid down in Annex III of the directive [DIR-1999-93-EC]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

4.3.11 P.Sig_Non-Repud (Non-repudiation of signatures)

SSCD CGA SCA

The lifecycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

4.4 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

[10] It is a non-qualified advanced electronic signature if it is based on a non-qualified certificate for the SVD.

4.4.1 A.Passive_Auth (PKI for Passive Authentication)

PACE EAC

The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document. The issuing State or Organisation runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer

(i) generates the Document Signer Key Pair,

(ii) hands over the Document Signer Public Key to the CA for certification,

(iii) keeps the Document Signer Private Key secret and

(iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents.

The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organisations. It is assumed that the Personalisation Agent ensures that the Document Security Object contains only the hash values of genuine user data according to [ICAO-9303-2015].

4.4.2 A.Insp_Sys (Inspection Systems for global interoperability)

EAC

The Extended Inspection System (EIS) for global interoperability

(i) includes the Country Signing CA Public Key and

(ii) implements the terminal part of PACE [ICAO-TR-110] and/or BAC [BSI-CC-PP-0055-110].

BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The *EIS* reads the logical travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. **If PACE Chip Authentication Mapping is used, Chip Authentication v.1 may be skipped**[11]. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data. **Optionally the Inspection Systems implements Active Authentication.**[12]

Justification: The assumption A.Insp_Sys does not confine the security objectives of the [BSI-CC-PP-0068-V2-2011-MA-01] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the the EAC functionality of the TOE.

4.4.3 A.Auth_PKI (PKI for Inspection Systems)

EAC

The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organisations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their travel document's chip.

[11] since Chip Authentication functionally is part of PACE Chip Authentication Mapping
[12] cf. [BSI-TR-03110-1-V220], section 2.4

Justification: This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the [BSI-CC-PP-0068-V2-2011-MA-01] be restricted by this assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication Protocol Version 1.

4.4.4 A.CGA (Trustworthy certificate generation application)

SSCD *CGA* *SCA*

The CGA protects the authenticity of the signatory's name or pseudonym and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP.

4.4.5 A.SCA (Trustworthy signature creation application)

SSCD *CGA* *SCA*

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of the data the signatory wishes to sign in a form appropriate for signing by the TOE.

4.4.6 A.Env_Admin (Environment for administrator)

TOE initialization, TOE personalization by the Administrator only takes place within a trusted environment.

eSign update (generation of SCD/SVD pair, export of SVD and optional creation/update of EFs / DFs) is performed by the Administrator through a trusted channel as a trusted environment.

Notes

1. "A.Env_Admin" is added to the security problem definitions of the claimed protection profiles.
2. For initialization and personalization both TOE and Administrator reside in a trusted environment.
3. For eSign update the administrator resides in a trusted environment.
4. After authentication and trusted channel establishment communication via trusted channel is considered to be a trusted environment.

4.4.7 A.Env_Mass_Signature (Environment for a mass signature TOE)

Mass signature generation only takes place within a trusted environment.

Notes

1. "A.Env_Mass_Signature" is added to the security problem definitions of the claimed protection profiles.
2. Trusted Environment means for mass signature generation a physically trusted environment.

---

5 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.

5.1 Security Objectives for the TOE

The following TOE security objectives address the protection provided by the TOE *independent* of the TOE environment.

5.1.1 OT.Data_Integrity (Integrity of Data)

PACE EAC

The TOE must ensure integrity of the User Data and the TSF-data[1] stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying). The TOE must ensure integrity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

Notes

1. OT.Data_Integrity holds also for Extended Inspection System which has used an authenticated BIS-PACE for authentication.

5.1.2 OT.Data_Authenticity (Authenticity of Data)

PACE EAC

The TOE must ensure authenticity of the User Data and the TSF-data[2] stored on it by enabling verification of their authenticity at the terminal-side[3] . The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE)[4].

Notes

1. REFINEMENT OT.Data_Authenticity holds also for Extended Inspection System which has used an authenticated BIS-PACE for authentication.

[1] where appropriate, see [BSI-CC-PP-0068-V2-2011-MA-01], Table 2
[2] where appropriate, see [BSI-CC-PP-0068-V2-2011-MA-01], Table 2
[3] verification of SO_D
[4] secure messaging after the PACE authentication, see also [ICAO-TR-110]

5.1.3 OT.Data_Confidentiality (Confidentiality of Data)

PACE EAC

The TOE must ensure confidentiality of the User Data and the TSF-data[5] by granting read access only to the PACE authenticated BIS-PACE connected. The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

Note

1. REFINEMENT OT.Data_Confidentiality holds also for Extended Inspection System which has used an authenticated BIS-PACE for authentication.

5.1.4 OT.Tracing (Tracing travel document)

PACE EAC

The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless/contact interface of the TOE without knowledge of the correct values of shared passwords (PACE passwords) in advance.

5.1.5 OT.Prot_Abuse-Func (Protection against Abuse of Functionality)

PACE EAC

The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (#) to manipulate or to disclose the TSF-data stored in the TOE, (#) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

5.1.6 OT.Prot_Inf_Leak (Protection against Information Leakage)

PACE EAC

The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the travel document

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

Note

1. This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker (cf. application note 22 of [BSI-CC-PP-0068-V2-2011-MA-01]).

---

[5] where appropriate, see [BSI-CC-PP-0068-V2-2011-MA-01], Table 2

5.1.7 OT.Prot_Phys-Tamper (Protection against Physical Tampering)

PACE *EAC*

The TOE must provide protection of confidentiality and integrity of the User Data, the TSF-data and the travel document's Embedded Software by means of

- measuring through galvanic contacts representing a direct physical probing on the chip's surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts, but other types of physical interaction between electrical charges (using tools used in solid-state physics research and IC failure analysis),
- manipulation of the hardware and its security functionality, as well as
- controlled manipulation of memory contents (User Data, TSF-data)

with a prior

- reverse-engineering to understand the design and its properties and functionality.

5.1.8 OT.Prot_Malfunction (Protection against Malfunctions)

PACE *EAC*

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.

The following two TOE security objectives (OT.Identification and OT.AC_Pers) address the aspects of identified threats to be countered involving TOE's environment.

5.1.9 OT.Identification (Identification of the TOE)

PACE *EAC*

The TOE must provide means to store Initialisation[6] and Pre-Personalisation Data in its non-volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the travel document. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

Note

1. The OT.AC_Pers implies that the data of the LDS groups written during personalization for travel document holder (at least EF.DG1 and EF.DG2) cannot be changed using write access after personalization. (cf. application note 23 of [BSI-CC-PP-0068-V2-2011-MA-01]).

---

[6] amongst other, IC Identification data

5.1.10 OT.AC_Pers (Access Control for Personalisation of logical MRTD)

PACE EAC

The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [ICAO-9303-2015] and the TSF data can be written by authorized Personalisation Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalisation of the document.

5.1.11 OT.Sens_Data_Conf (Confidentiality of sensitive biometric reference data)

EAC

The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organisation. The TOE must ensure the confidentiality of the logical travel document data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

5.1.12 OT.Chip_Auth_Proof (Proof of the travel document's chip authenticity)

EAC

The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organisation by means of the Chip Authentication Version 1 as defined in [BSI-TR-03110-1-V220] and by means of PACE *Chip Authentication Mapping* as defined in [ICAO-TR-110], [BSI-TR-03110-1-V220]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

Note

The OT.Chip_Auth_Proof implies the travel document's chip to have

(i) a unique identity as given by the travel document's Document Number,

(ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data.

The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of travel document's chip i.e.

- in the case of Chip Authentication v.1: a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip. This certificate is provided by
  (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [ICAO-9303-2015] and
  (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.
- in the case of PACE Chip Authentication Mapping: a certificate for the Public Key that matches the PACE-CAM Private Key of the travel document's chip. This certificate is provided by
  (i) the Public Key (EF.CardSecurity) in the LDS defined in [ICAO-TR-110] and

(ii) the hash value of EF.CardSecurity in the Document Security Object signed by the Document Signer.

5.1.13 OT.AA_Proof (Proof of the travel document's chip authenticity)

The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [ICAO-9303-2015].The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.[7]

5.1.14 OT.Lifecycle_Security (Lifecycle security)

SSCD *CGA* *SCA*

The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall securely destroy the SCD on demand of the signatory.

Note

1. This TOE can contain several SCDs (RSA or EC based). There is no need to destroy the SCD in case of repeated SCD generation. The signatory shall be able to destroy the SCD stored in the SSCD, e.g. after the (qualified) certificate for the corresponding SVD has been expired.

5.1.15 OT.SCD/SVD_Auth_Gen (Authorised SCD/SVD generation)

SSCD *CGA* *SCA*

The TOE shall provide security features to ensure that authorised users only may invoke the generation of the SCD and the SVD.

Note

1. This objective is defined in [BSI-CC-PP-0059-2009-MA-02] as *OT.SCD/SVD_Auth_Gen* and referenced by [BSI-CC-PP-0071-2012-MA-01] and [BSI-CC-PP-0072-2012-MA-01] as *OT.SCD/SVD_Auth_Gen*.

5.1.16 OT.SCD_Unique (Uniqueness of the signature creation data)

SSCD *CGA* *SCA*

The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation shall practically occur only once and shall not be reconstructable from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible.

[7] REFINEMENT

5.1.17 OT.SCD_SVD_Corresp (Correspondence between SVD and SCD)

SSCD CGA SCA

The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating an electronic signature creation with the SCD.

5.1.18 OT.SCD_Secrecy (Secrecy of the signature creation data)

SSCD CGA SCA

The secrecy of the SCD (used for signature creation) shall be reasonably assured against attacks with a high attack potential.

Note

1. The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD/SVD generation, signature creation operation, storage and secure destruction.

5.1.19 OT.Sig_Secure (Cryptographic security of the electronic signature)

SSCD CGA SCA

The TOE shall create digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD shall not be reconstructable using the digital signatures or any other data exportable from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

5.1.20 OT.Sigy_SigF (Signature creation function for the legitimate signatory only)

SSCD CGA SCA

The TOE shall provide the digital signature creation function for the legitimate signatory only and protects the SCD against the use of others. The TOE shall resist attacks with high attack potential.

5.1.21 OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE)

SSCD CGA SCA

The TOE shall not alter the DTBS/R. As by definition of the DTBS/R this may consist of the DTBS themselves, this objective does not conflict with a signature creation process where the TOE hashes the provided DTBS (in part or entirely) for signature creation.

5.1.22 OT.EMSEC_Design (Provide physical emanations security)

SSCD CGA SCA

The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits.

5.1.23 OT.Tamper_ID (Tamper detection)

SSCD CGA SCA

The TOE shall provide system features that detect physical tampering of its components, and uses those features to limit security breaches.

5.1.24 OT.Tamper_Resistance (Tamper resistance)

SSCD CGA SCA

The TOE shall prevent or resist physical tampering with specified system devices and components.

5.1.25 OT.TOE_SSCD_Auth (Authentication proof as SSCD)

CGA

The TOE shall hold unique identity and authentication data as SSCD and provide security mechanisms to identify and to authenticate itself as SSCD.

Note

1. This security objective only applies in case a communication channel to the CGA (via trusted channel) in the Life Cycle Phase "Usage/Operational" is needed.

5.1.26 OT.TOE_TC_SVD_Exp (TOE trusted channel for SVD export)

CGA

The TOE shall provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA. The TOE shall enable the CGA to detect alteration of the SVD exported by the TOE.

Note

1. This security objective only applies for the Life Cycle Phase "Usage/Operational" as the TOE provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase "Usage/Operational".

5.1.27 OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import)

SCA

The TOE shall provide a trusted channel for the protection of the confidentiality and integrity of the VAD received from the HID as needed by the authentication method employed.

Notes

1. This security objective for the TOE is partly covering *OE.HID_VAD (Protection of the VAD)* from [BSI-CC-PP-0059-2009-MA-02]. While OE.HID_VAD in [BSI-CC-PP-0059-2009-MA-02] requires only the operational environment to protect VAD, [BSI-CC-PP-0072-2012-MA-01] requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to *OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD export)*, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore [BSI-CC-PP-0072-2012-MA-01] re-assigns partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

5.1.28 OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS import)

SCA

The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS/R received from the SCA. The TOE shall not generate electronic signatures with the SCD for altered DTBS.

Notes

1. This security objective for the TOE is partly covering OE.DTBS_Protect from [BSI-CC-PP-0059-2009-MA-02]. While OE.DTBS_Protect in [BSI-CC-PP-0059-2009-MA-02] requires only the operational environment to protect DTBS, [BSI-CC-PP-0072-2012-MA-01] requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, [BSI-CC-PP-0072-2012-MA-01] TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore PP re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

5.2 Security Objectives for the Operational Environment

Travel document Issuer as the general responsible

The travel document Issuer as the general responsible for the global security policy related will implement the following security objectives for the TOE environment:

5.2.1 OE.Legislative_Compliance (Issuing of the travel document)

PACE
EAC

The travel document Issuer must issue the travel document and approve it using the terminals complying with all applicable laws and regulations.

Travel document Issuer and CSCA: travel document's PKI (issuing) branch

The travel document Issuer and the related CSCA will implement the following security objectives for the TOE environment: (see also the note in the definition of *P.Card_PKI (PKI for Passive Authentication (issuing branch))* above)

5.2.2 OE.Passive_Auth_Sign (Authentication of travel document by Signature)

PACE
EAC

The travel document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must

(i) generate a cryptographically secure CSCA Key Pair,

(ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and

(iii) publish the Certificate of the CSCA Public Key (C_{CSCA}).

Hereby authenticity and integrity of these certificates are being maintained.

A Document Signer acting in accordance with the CSCA policy must

(i) generate a cryptographically secure Document Signing Key Pair,

(ii) ensure the secrecy of the Document Signer Private Key,

(iii) hand over the Document Signer Public Key to the CSCA for certification,

(iv) sign Document Security Objects of genuine travel documents in a secure operational environment only.

The digital signature in the Document Security Object relates to all hash values for each data group in use according to [6]. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [6]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.

5.2.3 OE.Personalisation (Personalisation of travel document)

The travel document Issuer must ensure that the Personalisation Agents acting on his behalf *PACE EAC*

(i) establish the correct identity of the travel document holder and create the biographical data for the travel document,

(ii) enrol the biometric reference data of the travel document holder,

(iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder as defined in [ICAO-9303-2015][8],

(iv) write the document details data,

(v) write the initial TSF data,

(vi) sign the Document Security Object defined in [ICAO-9303-2015] (in the role of a DS).

Terminal operator: Terminal's receiving branch

5.2.4 OE.Terminal (Terminal operating)

The terminal operators must operate their terminals as follows: *PACE EAC*

1) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [ICAO-9303-2015].

2) The related terminals implement the terminal parts of the PACE protocol [ICAO-TR-110], of the Passive Authentication [ICAO-TR-110] (by verification of the signature of the Document Security Object) and use them in this order[9]. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

3) The related terminals need not to use any own credentials.

4) The related terminals securely 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 of the travel document (determination of the authenticity of data groups stored in the travel document, [ICAO-9303-2015]).

5) The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current PP.

Note

[8] see also [ICAO-9303-2015], part 10

[9] This order is commensurate with [ICAO-TR-110].

1. OE.Terminal completely covers and extends "OE.Exam_MRTD", "OE.Passive_Auth_Verif" and "OE.Prot_Logical_MRTD" from BAC PP [BSI-CC-PP-0055-110]. (cf. application note 24 of [BSI-CC-PP-0068-V2-2011-MA-01]).

Travel document holder Obligations

5.2.5 OE.Travel_Document_Holder (Travel document holder Obligations)

PACE *EAC*

The travel document holder may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device who definitely act according to respective regulations and are trustworthy.

Issuing State or Organisation

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

5.2.6 OE.Auth_Key_Travel_Document (Travel document Authentication Key)

EAC

The issuing State or Organisation has to establish the necessary public key infrastructure in order to

(i) generate the travel document's Chip Authentication Key Pair,

(ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and

(iii) support inspection systems of receiving States or Organisations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the Chip Authentication Public Key by means of the Document Security Object.

5.2.7 OE.AA_Key_Travel_Document (Travel document Authentication Key)

The issuing State or Organization has to establish the necessary public key infrastructure in order to

(i) generate the travel document's Active Authentication Key Pair,

(ii) sign and store the Active Authentication Public Key data in EF.DG15 and

(iii) support inspection systems of receiving States or Organizations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the Active Authentication Public Key by means of the Document Security Object.[10]

[10] REFINEMENT

5.2.8 OE.Authoriz_Sens_Data (Authorization for Use of Sensitive Biometric Reference Data)

EAC

The issuing State or Organisation has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of travel document holders to authorized receiving States or Organisations. The Country Verifying Certification Authority of the issuing State or Organisation generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

Receiving State or Organisation

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

5.2.9 OE.Exam_Travel_Document (Examination of the physical part of the travel document)

EAC

The inspection system of the receiving State or Organisation must examine the travel document presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability

(i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organisation, and

(ii) implements the terminal part of PACE [ICAO-TR-110] and/or the Basic Access Control [ICAO-9303-2015].

Extended Inspection Systems perform additionally to these points the PACE *Chip Authentication Mapping* or/and Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.

OE.Exam_Travel_Document also repeats partly the requirements from OE.Terminal in [BSI-CC-PP-0068-V2-2011-MA-01] and therefore also counters T.Forgery and A.Passive_Auth from [BSI-CC-PP-0068-V2-2011-MA-01] . This is done because a new type of Inspection System is introduced in this PP as the Extended Inspection System is needed to handle the additional features of a travel document with Extended Access Control.

Inspection Systems not able to perform EAC perform additionally to these points Active Authentication (if optionally available and the terminal's ability allows to perform AA) to verify the Authenticity of the presented travel document's chip.[11]

5.2.10 OE.Prot_Logical_Travel_Document (Protection of data from the logical travel document)

EAC

The inspection system of the receiving State or Organisation ensures the confidentiality and integrity of the data read from the logical travel document. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol Version 1.

[11] REFINEMENT

5.2.11 OE.Ext_Insp_Systems (Authorization of Extended Inspection Systems)

EAC

The Document Verifier of receiving States or Organisations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical travel document. The Extended Inspection System authenticates themselves to the travel document's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.

Environmental security objectives for SSCD

5.2.12 OE.SVD_Auth (Authenticity of the SVD)

SSCD
CGA
SCA

The operational environment shall ensure the integrity of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

5.2.13 OE.CGA_QCert (Generation of qualified certificates)

SSCD
CGA
SCA

The CGA shall generate a qualified certificate that includes (amongst others):

a) the name of the signatory controlling the TOE;

b) the SVD matching the SCD stored in the TOE and being under sole control of the signatory;

c) the advanced signature of the CSP.

The CGA shall confirm with the generated qualified certificate that the SCD corresponding to the SVD is stored in a SSCD.

5.2.14 OE.SSCD_Prov_Service (Authentic SSCD provided by SSCD-provisioning service)

SSCD
SCA

The SSCD-provisioning service shall initialise and personalise for the signatory an authentic copy of the TOE and deliver this copy as SSCD to the signatory.

5.2.15 OE.HID_VAD (Protection of the VAD)

SSCD
CGA

If an external device provides the human interface for user authentication, this device shall ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface. In particular, if the TOE requires a trusted channel for import of the VAD, the HID shall support usage of this trusted channel.

5.2.16 OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD export)

SCA

The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel.

Notes

1. This security objective for the TOE is partly covering *OE.HID_VAD (Protection of the VAD)* from the core [BSI-CC-PP-0059-2009-MA-02]. While OE.HID_VAD in [BSI-CC-PP-0059-2009-MA-02] requires only the operational environment to protect VAD, [BSI-CC-PP-0072-2012-MA-01] requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to *OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import)*. Therefore [BSI-CC-PP-0072-2012-MA-01] re-assigns partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

5.2.17 OE.DTBS_Intend (SCA sends data intended to be signed)

SSCD
CGA
SCA

The signatory shall use a trustworthy SCA that:

- generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE;
- sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE;
- attaches the signature produced by the TOE to the data or provides it separately.

Note

1. The SCA should be able to support advanced electronic signatures. Currently, there are three formats defined by ETSI recognized as meeting the requirements needed by advanced electronic signatures: CadES, XadES and PadES. These three formats mandate to include the hash of the signer's public key certificate in the data to be signed. In order to support for the mobility of the signer, it is recommended to store the certificate info on the SSCD for use by SCA and identification of the corresponding SCD if more than one SCD is stored on the SSCD.

5.2.18 OE.DTBS_Protect (SCA protects the data intended to be signed)

SSCD
CGA

The operational environment shall ensure that the DTBS/R cannot be altered in transit between the SCA and the TOE. In particular, if the TOE requires a trusted channel for import of the DTBS/R, the SCA shall support usage of this trusted channel.

5.2.19 OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS export)

SCA

The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE.

Notes

1. This security objective for the TOE is partly covering *OE.DTBS_Protect (SCA protects the data intended to be signed)* from the core [BSI-CC-PP-0059-2009-MA-02]. While OE.DTBS_Protect in [BSI-CC-PP-0059-2009-MA-02] requires only the operational environment to protect DTBS, [BSI-CC-PP-0072-2012-MA-01] requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA

exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to *OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS import)*. Therefore [BSI-CC-PP-0072-2012-MA-01] re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

5.2.20 OE.Signatory (Security obligation of the signatory)

SSCD
CGA
SCA

The signatory shall check that the SCD stored in the SSCD received from SSCD-provisioning service is in non-operational state. The signatory shall keep their VAD confidential.

Note

1. The signatory may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device (PACE Terminal) who are trustworthy.

5.2.21 OE.Dev_Prov_Service (Authentic SSCD provided by SSCD Provisioning Service)

CGA

The SSCD Provisioning Service handles authentic devices that implement the TOE, prepares the TOE for proof as SSCD to external entities, personalizes the TOE for the legitimate user as signatory, links the identity of the TOE as SSCD with the identity of the legitimate user, and delivers the TOE to the signatory.

NOTE

This objective replaces *OE.SSCD_Prov_Service (Authentic SSCD provided by SSCD-provisioning service)* from the core PP, which is possible as it does not imply any additional requirements for the operational environment when compared to OE.SSCD_Prov_Service (OE.Dev_Prov_Service is a subset of OE.SSCD_Prov_Service).

2. The preparation of the TOE for proof as SSCD to external entities only applies in case a communication channel to the CGA (via trusted channel) in the Life Cycle Phase "Usage/Operational" is needed.

5.2.22 OE.CGA_SSCD_Auth (Pre-initialization of the TOE for SSCD authentication)

CGA

The CSP shall check by means of the CGA whether the device presented for application of a (qualified) certificate holds unique identification as SSCD, successfully proved this identity as SSCD to the CGA, and whether this identity is linked to the legitimate holder of the device as applicant for the certificate.

Note

1. This security objective only applies in case a communication channel to the CGA (via trusted channel) in the Life Cycle Phase "Usage/Operational" is needed.

5.2.23 OE.CGA_TC_SVD_Imp (CGA trusted channel for SVD import)

CGA

The CGA shall detect alteration of the SVD imported from the TOE with the claimed identity of the SSCD.

The developer prepares the TOE by pre-initialization for the delivery to the customer (i.e. the SSCD provisioning service) in the development phase not addressed by a security objective for the operational environment. The SSCD Provisioning Service performs initialization and personalization as TOE for the legitimate user (i.e. the Device holder). If the TOE is delivered to the Device holder with SCD the TOE is a SSCD. This situation is addressed by *OE.SSCD_Prov_Service (Authentic SSCD provided by SSCD-provisioning service)* except the additional initialization of the TOE for proof as SSCD and trusted channel to the CGA. If the TOE is delivered to the Device holder without a SCD the TOE will be a SSCD only after generation of the first SCD/SVD pair. Because this SCD/SVD pair generation is performed by the signatory in the Phase "Usage/Operational" the TOE provides additional security functionality addressed by *OT.TOE_SSCD_Auth (Authentication proof as SSCD)* and *OT.TOE_TC_SVD_Exp (TOE trusted channel for SVD export)*. But this security functionality shall be initialized by the SSCD Provisioning Service as described in OE.Dev_Prov_Service. Therefore [BSI-CC-PP-0071-2012-MA-01] substitutes OE.SSCD_Prov_Service by OE.Dev_Prov_Service allowing generation of the first SCD/SVD pair after delivery of the TOE to the Device holder and requiring initialization of security functionality of the TOE. Nevertheless the additional security functionality shall be used by the operational environment as described in OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp. This approach does not weaken the security objectives of and requirements to the TOE but enforce more security functionality of the TOE for additional method of use. Therefore it does not conflict with the CC conformance claim to the core [BSI-CC-PP-0059-2009-MA-02] .

Note

1. This security objective only applies for the Life Cycle Phase "Usage/Operational" as the TOE provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase "Usage/Operational".

5.2.24 OE.Env_Admin (Administrator works in trusted environment)

The administrative functions of "Administrator" users are performed within a trusted environment.

Notes

1. "OE.Env_Admin" is added to the contents of the claimed protection profiles.
2. After authentication and trusted channel establishment communication via trusted channel is considered to be a trusted environment.

1760 ### 5.2.25 OE.Env_Mass_Signature (Mass signatures are generated in-trusted environment only)

Mass signature generation only takes place within a trusted environment.

Note

1765 1. “OE.Env_Mass_Signature” is added to the contents of the claimed protection profiles.

5.3 Security Objective Rationale

5.3.1 Security Objectives Backtracking

Fig. 5.1 shows that

- all threats and OSPs are addressed by the security objectives and
1770 - that all assumptions are addressed by the security objectives for the TOE environment.

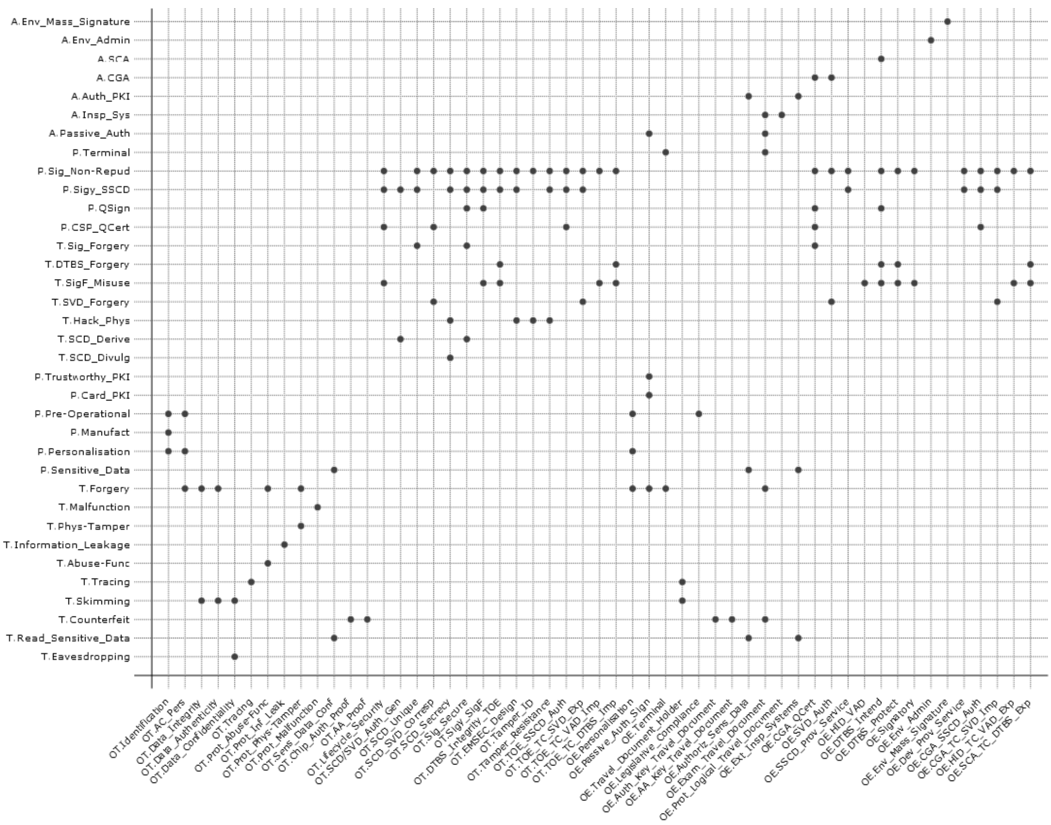

Fig. 5.1: Security Objective Rationale overview

5.3.2 Security Objectives Sufficiency

Countering of threats by security objectives

SSCD

T.SCD_Divulg (Storing, copying and releasing of the signature creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in **the Directive**, recital (18). This threat is countered by

- *OT.SCD_Secrecy (Secrecy of the signature creation data)*, which assures the secrecy of the SCD used for signature creation.

SSCD

T.SCD_Derive (Derive the signature creation data) deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD.

- *OT.SCD/SVD_Auth_Gen (Authorised SCD/SVD generation)* counters this threat by implementing cryptographically secure generation of the SCD/SVD pair.
- *OT.Sig_Secure (Cryptographic security of the electronic signature)* ensures cryptographically secure electronic signatures.

SSCD

T.Hack_Phys (Physical attacks through the TOE interfaces) deals with physical attacks exploiting physical vulnerabilities of the TOE.

- *OT.SCD_Secrecy (Secrecy of the signature creation data)* preserves the secrecy of the SCD.
- *OT.EMSEC_Design (Provide physical emanations security)* counters physical attacks through the TOE interfaces and observation of TOE emanations.
- *OT.Tamper_ID (Tamper detection)* and
- *OT.Tamper_Resistance (Tamper resistance)* counter the threat T.Hack_Phys by detecting and by resisting tampering attacks.

CGA

T.SVD_Forgery (Forgery of the signature verification data) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate[12]. T.SVD_Forgery is addressed by

- *OT.SCD_SVD_Corresp (Correspondence between SVD and SCD)*, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and
- *OE.SVD_Auth (Authenticity of the SVD)* that ensures the integrity of the SVD exported by the TOE to the CGA and verification of the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP.

  Additionally T.SVD_Forgery is addressed by

- *OT.TOE_TC_SVD_Exp (TOE trusted channel for SVD export)*, which ensures that the TOE sends the SVD in a verifiable form through a trusted channel to the CGA, as well as by
- *OE.CGA_TC_SVD_Imp (CGA trusted channel for SVD import)*, which provides verification of SVD authenticity by the CGA.

SSCD

T.SigF_Misuse (Misuse of the signature creation function of the TOE) addresses the threat of misuse of the TOE signature creation function to create SDO by others than the signatory to create an electronic signature on data for which the signatory has not expressed the intent to sign, as required by Annex III of **the Directive**, paragraph 1, literal (c).

[12] The TOE provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase "Usage/Operational".

- *OT.Lifecycle_Security (Lifecycle security)* requires the TOE to detect flaws during the initialization, personalization and operational usage including secure destruction of the SCD, which may be initiated by the signatory.
- *OT.Sigy_SigF (Signature creation function for the legitimate signatory only)* ensures that the TOE provides the signature creation function for the legitimate signatory only.
- *OE.DTBS_Intend (SCA sends data intended to be signed)* ensures that the SCA sends the DTBS/R only for data the signatory intends to sign.
- *OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE)* prevents the DTBS/R from alteration inside the TOE.
- *OE.Signatory (Security obligation of the signatory)* ensures that the signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the signatory becomes control over the SSCD. OE.Signatory ensures also that the signatory keeps their VAD confidential.

SCA

The combination of

- *OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS import)* and
- *OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS export)* counters the undetected manipulation of the DTBS during the transmission from the SCA to the TOE

If the SCA provides a human interface for user authentication, *OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD export)* requires the HID to protect the confidentiality and the integrity of the VAD as needed by the authentication method employed. The HID and the TOE will protect the VAD by a trusted channel between HID and TOE according to

- *OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD export)* and
- *OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import)*.
- *OE.DTBS_Protect (SCA protects the data intended to be signed)* counters manipulation of the DTBS during transmission over the channel between SCA and the TOE.
- *OE.HID_VAD (Protection of the VAD)* provides confidentiality and integrity of the VAD as needed by the authentication method employed.

SSCD

T.DTBS_Forgery (Forgery of the DTBS/R) addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function that does not represent the DTBS as presented to the signatory and for which the signature has expressed its intent to sign.

The TOE IT environment addresses T.DTBS_Forgery by the means of

- *OE.DTBS_Intend (SCA sends data intended to be signed)*, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE.

  The TOE counters this threat by the means of

- *OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE)* by ensuring the integrity of the DTBS/R inside the TOE.

SCA

  The threat *T.DTBS_Forgery (Forgery of the DTBS/R)* is addressed by the security objectives

  - *OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS import)* and
  - *OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS export)*, which ensure that the DTBS/R is sent through a trusted channel and cannot be altered undetected in transit between the SCA and the TOE.

The TOE IT environment addresses T.DTBS_Forgery by the means of

- *OE.DTBS_Protect (SCA protects the data intended to be signed)*, which ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE.

SSCD

T.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature.

- *OT.Sig_Secure (Cryptographic security of the electronic signature)*,
- *OT.SCD_Unique (Uniqueness of the signature creation data)* and
- *OE.CGA_QCert (Generation of qualified certificates)* address this threat in general.
- *OT.Sig_Secure (Cryptographic security of the electronic signature)* ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together.
- *OT.SCD_Unique (Uniqueness of the signature creation data)* and ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance.
- *OE.CGA_QCert (Generation of qualified certificates)* prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

PACE

T.Skimming (Skimming travel document / Capturing Card-Terminal Communication) addresses accessing the VAD (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless/contact interface. This threat is countered by the security objective

- *OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import)* through the PACE authentication.

The objective

- *OE.Signatory (Security obligation of the signatory)* ensures that a PACE session can only be established either by the legitimate user itself or by an authorised person or device (PACE Terminal), and, hence, cannot be captured by an attacker.

PACE

T.Skimming (Skimming travel document / Capturing Card-Terminal Communication), *T.Eavesdropping (Eavesdropping on the communication between the TOE and the PACE terminal)*, *T.Tracing (Tracing travel document)*, are countered exactly by the same objectives according to the rationale in the protection profile [BSI-CC-PP-0068-V2-2011-MA-01].

EAC

The threat *T.Forgery (Forgery of Data)* addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the terminal. Additionally to the security objectives from PACE PP [BSI-CC-PP-0068-V2-2011-MA-01] which counter this threat, the examination of the presented MRTD passport book according to *OE.Exam_Travel_Document (Examination of the physical part of the travel document)* shall ensure its authenticity by means of the physical security measures and detect any manipulation of the physical part of the travel document.

PACE

T.Abuse-Func (Abuse of Functionality), *T.Information_Leakage (Information Leakage from travel document)*, *T.Phys-Tamper (Physical Tampering)*, and *T.Malfunction (Malfunction due to Environmental Stress)* are countered directly by one security objective namely OT.Prot_Abuse-Func, OT.Prot_Inf_Leaka, OT.Prot_Phys-Tamper, and OT.Malfunction respectively all in direct correspondence to [BSI-CC-PP-0068-V2-2011-MA-01].

EAC

T.Read_Sensitive_Data (Read the sensitive biometric reference data) is countered by OT.Sens_Data_Conf, OE.Ext_Insp_Systems, and OE.Authorized_Sens_Data in direct correspondence to [BSI-CC-PP-0068-V2-2011-MA-01].

The threat *T.Counterfeit (Counterfeit of travel document chip data)* addresses the attack of unauthorized copy or reproduction of the genuine travel document's chip. This attack is thwarted by chip an identification and authenticity proof required by *OT.Chip_Auth_Proof (Proof of the travel document's chip authenticity)* using an authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 or, for PACE *Chip Authentication Mapping*, to EF.CardSecurity and signed by means of Documents Security Objects as demanded by *OE.Auth_Key_Travel_Document (Travel document Authentication Key)*. According to *OE.Exam_Travel_Document (Examination of the physical part of the travel document)* the General Inspection system has to perform PACE *Chip Authentication Mapping* or the Chip Authentication Protocol Version 1 to verify the authenticity of the travel document's chip.

Please note that the paragraph "The threat *T.Counterfeit (Counterfeit of travel document chip data)*. . . " **above is copied due to optional Active Authentication because a refined copy can be read easier**.

The threat *T.Counterfeit (Counterfeit of travel document chip data)* addresses the attack of unauthorized copy or reproduction of the genuine travel document's chip. This attack is thwarted by chip an identification and authenticity proof required by *OT.AA_Proof (Proof of the travel document's chip authenticity)*[13] using an authentication key pair to be generated by the issuing State or Organization. The Public **Active**[14] Authentication Key has to be written into **EF.DG15**[15] and signed by means of Documents Security Objects as demanded by *OE.AA_Key_Travel_Document (Travel document Authentication Key)*[16]. According to *OE.Exam_Travel_Document (Examination of the physical part of the travel document)* the General Inspection system has to perform the **Active Authentication Protocol**[17] to verify the authenticity of the travel document's chip.

Enforcement of OSPs by security objectives

CGA

P.CSP_QCert (Qualified certificate) provides that the TOE and the SCA may be employed to sign data with (qualified) electronic signatures, as defined by **the Directive**, Article 5, paragraph 1. the Directive, recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The

- *OE.CGA_QCert (Generation of qualified certificates)* addresses the requirement of qualified (or advanced) electronic signatures as being based on qualified (or non-qualified) certificates.

According to

- *OT.TOE_SSCD_Auth (Authentication proof as SSCD)* the copies of the TOE will hold unique identity and authentication data as SSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as SSCD to prove this identity as SSCD to the CGA[18].
- The *OE.CGA_SSCD_Auth (Pre-initialization of the TOE for SSCD authentication)* ensures that the SP checks the proof of the device presented of the applicant that it is a SSCD[19].
- The *OT.SCD_SVD_Corresp (Correspondence between SVD and SCD)* ensures that the SVD exported by the TOE to the CGA corresponds to the SCD stored in the TOE and used by the signatory.
- The *OT.Lifecycle_Security (Lifecycle security)* ensures that the TOE detects flaws during the initialization, personalization and operational usage.

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate.

[13] REFINEMENT OT.Chip_Auth_Proof
[14] REFINEMENT Chip
[15] REFINEMENT EF.DG14
[16] OE.Auth_Key_Travel_Document
[17] Chip Authentication Protocol Version 1
[18] This security objective only applies in case a communication channel to the CGA (via trusted channel) in the Life Cycle Phase "Usage/Operational" is needed.
[19] This security objective only applies in case a communication channel to the CGA (via trusted channel) in the Life Cycle Phase "Usage/Operational" is needed.

- *OT.Sigy_SigF (Signature creation function for the legitimate signatory only)* ensures signatory's sole control of the SCD by requiring the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others.
- *OT.Sig_Secure (Cryptographic security of the electronic signature)* ensures that the TOE creates electronic signatures, which cannot be forged without knowledge of the SCD through robust encryption techniques.
- *OE.CGA_QCert (Generation of qualified certificates)* addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature.
- *OE.DTBS_Intend (SCA sends data intended to be signed)* ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

CGA SCA

P.Sigy_SSCD (TOE as secure signature creation device) requires the TOE to meet Annex III of **the Directive**. The paragraph 1(a) of Annex III of **the Directive** is ensured by

- *OT.SCD_Unique (Uniqueness of the signature creation data)* requiring that the SCD used for signature creation can practically occur only once.
- The *OT.SCD_Secrecy (Secrecy of the signature creation data)*, *OT.Sig_Secure (Cryptographic security of the electronic signature)* and *OT.EMSEC_Design (Provide physical emanations security)* and *OT.Tamper_Resistance (Tamper resistance)* address the secrecy of the SCD (cf. paragraph 1(a) of Annex III of the Directive).
- *OT.SCD_Secrecy (Secrecy of the signature creation data)* and *OT.Sig_Secure (Cryptographic security of the electronic signature)* meet the requirement in paragraph 1(b) of Annex III of the Directive by the requirements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE.
- *OT.Sigy_SigF (Signature creation function for the legitimate signatory only)* meets the requirement in paragraph 1(c) of Annex III of the Directive by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others.
- *OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE)* meets the requirements in paragraph 2 of Annex III of the Directive as the TOE shall not alter the DTBS/R.

The usage of SCD under sole control of the signatory is ensured by

- *OT.Lifecycle_Security (Lifecycle security)*,
- *OT.SCD/SVD_Auth_Gen (Authorised SCD/SVD generation)* and
- *OT.Sigy_SigF (Signature creation function for the legitimate signatory only)*.

OE.Dev_Prov_Service (Authentic SSCD provided by SSCD Provisioning Service) ensures that the legitimate user obtains a TOE sample as an authentic, initialized and personalized TOE from an SSCD Provisioning Service through the TOE delivery procedure.

If the TOE implements SCD generated under control of the SSCD Provisioning Service the legitimate user receives the TOE as SSCD. If the TOE is delivered to the legitimate user without SCD in the operational phase he or she applies for the (qualified) certificate as the Device holder and legitimate user of the TOE. The CSP will use the TOE security feature (addressed by the security objectives

- *OT.TOE_SSCD_Auth (Authentication proof as SSCD)* and
- *OT.TOE_TC_SVD_Exp (TOE trusted channel for SVD export)*) to check whether the device presented is a SSCD linked to the applicant

as required by

- *OE.CGA_SSCD_Auth (Pre-initialization of the TOE for SSCD authentication)* and the received SVD is sent by this SSCD as required by

- *OE.CGA_TC_SVD_Imp (CGA trusted channel for SVD import)*.

Thus the obligation of the SSCD provision service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside the secure preparation environment.

P.Sig_Non-Repud (Non-repudiation of signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in their certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensures the aspects of signatory's sole control over and responsibility for the electronic signatures created with the TOE.

- *OE.Dev_Prov_Service (Authentic SSCD provided by SSCD Provisioning Service)* ensures that the signatory uses an authentic TOE, initialized and personalized for the signatory.
- *OE.CGA_QCert (Generation of qualified certificates)* ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory.
- *OE.SVD_Auth (Authenticity of the SVD)* and
- *OE.CGA_QCert (Generation of qualified certificates)* require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory.
- *OT.SCD_SVD_Corresp (Correspondence between SVD and SCD)* ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE.
- *OT.SCD_Unique (Uniqueness of the signature creation data)* provides that the signatory's SCD can practically occur just once.
- *OE.Signatory (Security obligation of the signatory)* ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD-provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD).

The TOE security feature addressed by the security objectives ***CGA***

- **OT.TOE_SSCD_Auth and**
- **OT.TOE_TC_SVD_Exp supported by**
- **OE.Dev_Prov_Service**

enables the verification whether the device presented by the applicant is a SSCD as required by *OE.CGA_SSCD_Auth (Pre-initialization of the TOE for SSCD authentication)* **and the received SVD is sent by the device holding the corresponding SCD as required by** *OE.CGA_TC_SVD_Imp (CGA trusted channel for SVD import)*.

- *OT.Sigy_SigF (Signature creation function for the legitimate signatory only)* provides that only the signatory may use the TOE for signature creation. As prerequisite *OE.Signatory (Security obligation of the signatory)* ensures that the signatory keeps their VAD confidential.

The robust cryptographic techniques required by *OT.Sig_Secure (Cryptographic security of the electronic signature)* ensure that only this SCD may create a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification.

- *OT.Lifecycle_Security (Lifecycle security)*,
- *OT.SCD_Secrecy (Secrecy of the signature creation data)*,
- *OT.EMSEC_Design (Provide physical emanations security)*,
- *OT.Tamper_ID (Tamper detection)* and

- *OT.Tamper_Resistance (Tamper resistance)* protect the SCD against any compromise.

The confidentiality of VAD is protected during the transmission between the HI device and TOE according to

- *OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD export)* and
- *OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import)*.
- *OE.DTBS_Intend (SCA sends data intended to be signed)*,
- *OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE)*,
- *OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS export)* and
- *OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS import)* ensure that the TOE generates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS.
- *OE.DTBS_Intend (SCA sends data intended to be signed)*,
- *OE.DTBS_Protect (SCA protects the data intended to be signed)* and
- *OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE)* ensure that the TOE creates electronic signatures only for those DTBS/R, which the signatory has decided to sign as DTBS.

P.Manufact (Manufacturing of the travel document's chip) is covered directly by *OT.Identification (Identification of the TOE)* since the objective mandates that the TOE implements identification mechanisms that support the identification of the TOE during manufacturing.

PACE

P.Pre-Operational (Pre-operational handling of the travel document) is enforced by the security objectives:

- *OT.Identification (Identification of the TOE)*
- *OT.AC_Pers (Access Control for Personalisation of logical MRTD)*
- *OE.Personalisation (Personalisation of travel document)*
- and *OE.Legislative_Compliance (Issuing of the travel document)*

in direct correspondence to the protection profile [BSI-CC-PP-0068-V2-2011-MA-01].

PACE

P.Card_PKI (PKI for Passive Authentication (issuing branch)), *P.Trustworthy_PKI (Trustworthiness of PKI)*, and are each directly enforced by a single security objective, namely *OE.Passive_Auth_Sign (Authentication of travel document by Signature)*, *OE.Passive_Auth_Sign (Authentication of travel document by Signature)*, and in direct correspondence to the protection profile [BSI-CC-PP-0068-V2-2011-MA-01].

PACE

The *P.Terminal (Abilities and trustworthiness of terminals)* is countered by the security objective *OE.Exam_Travel_Document (Examination of the physical part of the travel document)* additionally to the security objectives from PACE PP [BSI-CC-PP-0068-V2-2011-MA-01]. *OE.Exam_Travel_Document (Examination of the physical part of the travel document)* enforces the terminals to perform the terminal part of the PACE protocol.

EAC

The OSP *P.Personalisation (Personalisation of the travel document by issuing State or Organisation only)* addresses the

(i) the enrolment of the logical travel document by the Personalization Agent as described in the security objective for the TOE environment *OE.Personalisation (Personalisation of travel document)*, and

(ii) the access control for the user data and TSF data as described by the security objective *OT.AC_Pers (Access Control for Personalisation of logical MRTD)*.

Note the manufacturer equips the TOE with the Personalization Agent Key(s) according to *OT.Identification (Identification of the TOE)*. The security objective *OT.AC_Pers (Access*

Control for Personalisation of logical MRTD) limits the management of TSF data and the management of TSF to the Personalization Agent.

EAC

The *P.Sensitive_Data (Privacy of sensitive biometric reference data)* is fulfilled and the threat *T.Read_Sensitive_Data (Read the sensitive biometric reference data)* is countered by the TOE-objective *OT.Sens_Data_Conf (Confidentiality of sensitive biometric reference data)* requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organization as required by *OE.Authoriz_Sens_Data (Authorization for Use of Sensitive Biometric Reference Data)* by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by *OE.Ext_Insp_Systems (Authorization of Extended Inspection Systems)*.

Upkeep of assumptions by security objectives

A.SCA (Trustworthy signature creation application) establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by

- *OE.DTBS_Intend (SCA sends data intended to be signed)* which ensures that the SCA generates the DTBS/R of the data that have been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE.

A.CGA (Trustworthy certificate generation application) establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by

- *OE.CGA_QCert (Generation of qualified certificates)*, which ensures the generation of qualified certificates, and by
- *OE.SVD_Auth (Authenticity of the SVD)*, which ensures the protection of the integrity of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

A.Env_Admin (Environment for administrator) establishes a trustworthy environment for the Administrator for setting up the initialization and personalization of the TOE after the Administrator is successfully authenticated. This is addressed by *OE.Env_Admin (Administrator works in trusted environment)* which ensures that the TOE initialization, TOE personalization is only started by the Administrator within a trusted environment and eSign update (generation of SCD/SVD pair, export of SVD and optional creation/update of EFs / DFs) is performed by the Administrator through a trusted channel as a trusted environment.

Notes

1. "A.Env_Admin" and "OE.Env_Admin" are added to the contents of [BSI-CC-PP-0059-2009-MA-02].
2. After authentication and trusted channel establishment communication via trusted channel is considered to be a trusted environment.

A.Env_Mass_Signature (Environment for a mass signature TOE) establishes a trustworthy environment for the signatory for generating mass signatures after the signatory is successfully authenticated. This is addressed by OE.Env_Mass_Signature (Mass signatures are generated in trusted environment only) which ensures that generation of mass signatures takes place only in a trusted environment.

Note

1. "A.Env_Mass_Signature " and "OE.Env_Mass_Signature " are added to the contents of [BSI-CC-PP-0059-2009-MA-02].

The examination of the travel document addressed by the assumption *A.Insp_Sys (Inspection Systems for global interoperability)* is covered by the security objectives for the TOE environment *OE.Exam_Travel_Document (Examination of the physical part of the travel document)* which requires the inspection system to examine physically the travel document, the Basic Inspection System to implement the Basic Access Control, and the Extended Inspection Systems to implement and to perform PACE *Chip Authentication Mapping* or the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip. The security objectives for the TOE environment *OE.Prot_Logical_Travel_Document (Protection of data from the logical travel document)* require the Inspection System to protect the logical travel document data during the transmission and the internal handling. **"Travel document Authentication Key"**.[20]

The assumption *A.Passive_Auth (PKI for Passive Authentication)* is directly covered by the security objective for the TOE environment *OE.Passive_Auth_Sign (Authentication of travel document by Signature)* from PACE PP [BSI-CC-PP-0068-V2-2011-MA-01] covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by *OE.Exam_Travel_Document (Examination of the physical part of the travel document)*.

The assumption *A.Auth_PKI (PKI for Inspection Systems)* is covered by the security objective for the TOE environment *OE.Authoriz_Sens_Data (Authorization for Use of Sensitive Biometric Reference Data)* requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organizations only. The Document Verifier of the receiving State is required by *OE.Ext_Insp_Systems (Authorization of Extended Inspection Systems)* to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organization has to establish the necessary public key infrastructure.

[20] REFINEMENT

6 Extended Components Definition

This Security Target uses the components defined in

- chapter 5 of [BSI-CC-PP-0068-V2-2011-MA-01]
- chapter 5 of [BSI-CC-PP-0056-V2-2012-MA-02]

for the ePass and eID applications and

- chapter 8 of [BSI-CC-PP-0059-2009-MA-02]
- chapter 8 of [BSI-CC-PP-0071-2012-MA-01]
- chapter 8 of [BSI-CC-PP-0072-2012-MA-01]

for eSign applications.

No other components are used.

7 Security Requirements (ASE_REQ)

Common Criteria allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration. Each of these operations is used in this ST.

This Security Target performs the missing operations and considers the Application Notes given in [BSI-CC-PP-0056-V2-2012-MA-02], [BSI-CC-PP-0068-V2-2011-MA-01], [BSI-CC-PP-0059-2009-MA-02], [BSI-CC-PP-0071-2012-MA-01] and [BSI-CC-PP-0072-2012-MA-01].

The following conventions have been applied to the set of operations that may be applied to functional requirements:

- selections are indicated by **bold** text and by footnotes which lists the deleted text,
- assignments are indicated by **bold** text and by footnotes which lists the deleted text,
- iterations are indicated by appending a slash "/" with informative data following the component title (for example "/SHA-2") and
- refinements are indicated by **bold** text and by footnotes which identifies the refined text or by **bold** text and a leading [REFINEMENT] and in case of a longer section with a closing [END REFINEMENT].

If an operation of a security functional requirement has already been performed in the referenced PP(s) that is indicated by underlined text and by a footnote that states the operation.

If a security functional requirement is added to contents of PP [BSI-CC-PP-0059-2009-MA-02], this is described by a note which also states whether the SFR is "iterated" or "not iterated" from a PP SFR.

7.1 Elliptic curves used

This TOE uses the following elliptic curves:

1. for 256 bits:
   a) P-256 ([NIST-FIPS-186-4], chapter D.1.2.3 "Curve P-256", aka secp256r1 or prime256v1)
   b) brainpoolP256r1 ([RFC-5639-2010-03] chapter 3.4)
2. for 384 bits:
   a. P-384 ([NIST-FIPS-186-4], chapter D.1.2.4 "Curve P-384", aka secp384r1)
   b. brainpoolP384r1 ([RFC-5639-2010-03] chapter 3.6)
3. for 512 bits:

   brainpoolP512r1 ([RFC-5639-2010-03] chapter 3.7)
4. for 521 bits:

   P-521 ([NIST-FIPS-186-4], chapter D.1.2.5 "Curve P-521", aka secp521r1)

Notes

1. EC curves above are taken from [BSI-TR-03110-3-V221] Table 4: Standardized Domain Parameters.
2. This TOE uses the EC crypto library v2.08.007 of the underlying chip SLC52GDA448*.

3. For "ECDH" see [Infineon-ST-SLC52-H13] section "7.1.4.5.5 Elliptic Curve Diffie-Hellman (ECDH) key agreement".
4. For the "digital signature generation" see [Infineon-ST-SLC52-H13], "8.5.4 Elliptic Curves Cryptographic Library", section "Signature Generation and Verification".
5. For the "cryptographic key generation algorithm" see [Infineon-ST-SLC52-H13], "7.1.4.5.4 Elliptic Curve (EC) key generation"
6. For the "digital signature verification" see [Infineon-ST-SLC52-H13], "8.5.4 Elliptic Curves Cryptographic Library", section "ECDSA Signature Verification".

7.2 RSA key support

The TOE supports the following RSA key sizes:

- 2048, 3072, and 4096 bits

Both the straight-forward and the CRT key representation are supported. The straight-forward key representation for private keys is limited to the 2048bit representation.

Notes

1. This TOE uses the RSA crypto library v2.08.007 of the underlying chip SLC52GDA448*.
2. For "DH" the TOE uses the Modular Arithmetic Operations listed in [Infineon-ST-SLC52-H13], "8.5.3 RSA Cryptographic Library", section "Encryption, Decryption, Signature Generation and Verification".
3. For the "digital signature generation" see [Infineon-ST-SLC52-H13], "8.5.3 RSA Cryptographic Library", section "Encryption, Decryption, Signature Generation and Verification".
4. For the "cryptographic key generation algorithm" see [Infineon-ST-SLC52-H13], "7.1.4.5.2 Rivest-Shamir-Adleman (RSA) key generation"
5. For the "digital signature verification" see [Infineon-ST-SLC52-H13], "8.5.3 RSA Cryptographic Library", section "Encryption, Decryption, Signature Generation and Verification".

7.3 Hash functions implemented

This TOE provides the following hash algorithms

1. SHA-1
2. SHA-{256, 384, 512}.

Notes

1. This TOE uses for SHA-{1, 256, 384, 512} the SHA crypto library v1.12.001 of the underlying chip SLC52GDA448*.
2. For the implemented standards, see [Infineon-Chip-HCL52], "Annex D Reference list of implemented standards".

7.4 Security attributes

This ST defines the following security attributes for the PACE/EAC based access control:

Table 7.1: Terminal Authentication Status[1]

Value	Meaning
none (any terminal)	default role (i.e. without authorization after start-up)
CVCA	terminal is authenticated as *CVCA* after successful CA v.1 and TA v.1
DV (domestic)	terminal is authenticated as domestic *DV* after successful CA v.1 and TA v.1
DV (foreign)	terminal is authenticated as foreign *DV* after successful CA v.1 and TA v.1
IS	terminal is authenticated as *IS* after successful CA v.1 and TA v.1

Table 7.2: Terminal Authorization

Values	Meaning
none	
DG4 (Iris)	Read access to DG4 (cf. [BSI-TR-03110-4-V221] Table 2)
DG3 (Fingerprint)	Read access to DG3 (cf. [BSI-TR-03110-4-V221] Table 2)

Notes

1. Security attribute Terminal Authentication Status is spelled differently in PP [BSI-CC-PP-0056-V2-2012-MA-02], e.g. FDP_ACF.1/TRM spells it *Terminal Authentication v.1*.
2. Security attribute Terminal Authorization is spelled differently in PP [BSI-CC-PP-0056-V2-2012-MA-02], e.g. FDP_ACF.1/TRM spells it *Authorization of the Terminal*.
3. These diffent spellings are corrected by refinements to read always *Terminal Authentication Status* or *Terminal Authorization*.
4. A combination of Terminal Authorization attributes DG4 and DG3 is allowed and thus not not stated explicitly in Table 7.2.

The security attributes and related status for the subjects and objects for the SSCD related access control policy are:

Table 7.3: Security Attributes for SSCD related SFPs

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	authorized, not authorized
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)

[1] **REFINEMENT** terminal authentication status

7.5 Keys and certificates

Table 7.4 provide an overview of the keys and certificates used including further keys and certificates from [BSI-CC-PP-0068-V2-2011-MA-01].

Note:

1. Where PP [BSI-CC-PP-0068-V2-2011-MA-01] is more specific than PP [BSI-CC-PP-0056-V2-2012-MA-02] name and data are taken from the former.

Table 7.4: Keys and certificates

	Name	Data
	TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material by the TOE in order to enforce its security functionality.
receiving PKI branch	SK.CVCA	The Country Verifying Certification Authority (*CVCA*) holds a private key (SK.CVCA) used for signing the *DV* Certificates.
	PK.CVCA	The TOE stores the *CVCA* Public Key (PK.CVCA) as part of the TSF data to verify the *DV* Certificates. The PK.CVCA has the security attribute Current Date as the most recent valid effective date of the CVCA or of a domestic DV Certificate.
	C.CVCA	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [BSI-TR-03110-1-V220] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK.CVCA) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
	C.DV	The Document Verifier Certificate C.DV is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK.DV) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
	C.IS	The Inspection System Certificate (C.IS) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK.IS), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Issuing PKI branch	Chip Authentication key pair	The Chip Authentication key pair (SK.ICC, PK.ICC) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 11770-3 [ISO-IEC-11770-3].

continues on next page

Table 7.4 – continued from previous page

	Name	Data
	PK.ICC	The Chip Authentication Public Key (PK.ICC) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical travel document and used by the inspection system for Chip Authentication Version 1 of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.
	SK.ICC	The Chip Authentication Private Key (SK.ICC) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.
	Active Authentication key pair	The Active Authentication Key Pair (KPr.AA, KPu.AA) are used for Active Authentication Protocol according to [ICAO-9303-2015] part 11 chapter "6.1 Active Authentication)" using EC or RSA.
	KPu.AA	The Active Authentication Public Key (KPu.AA) is stored in the EF.DG15 of the TOE's logical travel document and used by the inspection system for Active Authentication of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.
	KPr.AA	The Active Authentication Private Key (KPr.AA) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.
	CSCA Key Pair and Certificate	*CSCA* of the travel document Issuer signs the Document Signer Public Key Certificate (C.DS) with the Country Signing Certification Authority Private Key (SK.CSCA) and the signature will be verified by receiving terminal with the Country Signing Certification Authority Public Key (PK.CSCA). The CSCA also issues the self-signed CSCA Certificate (CCSCA) to be distributed by strictly secure diplomatic means, see. [ICAO-9303-2015].
	DS Key Pairs and Certificates	The Document Signer Certificate C.DS is issued by the Country Signing Certification Authority. It contains the Document Signer Public Key (PK.DS) as authentication reference data. The Document Signer acting under the policy of the CSCA signs the Document Security Object (SO_D) of the travel document with the Document Signer Private Key (SK.DS) and the signature will be verified by a terminal as the Passive Authentication with the Document Signer Public Key (PK.DS).
	PACE Chip Authentication Mapping Public Key Pair	The PACE *Chip Authentication Mapping* Public Key Pair (SK.CAM, PK.CAM) are used for PACE *Chip Authentication Mapping* according to [ICAO-TR-110], [BSI-TR-03110-1-V220].

continues on next page

Table 7.4 – continued from previous page

	Name	Data
	PACE *Chip Authentication Mapping* Public Key (PK.CAM)	The PACE *Chip Authentication Mapping* Public Key (PK.CAM) is stored in the EF.CardSecurity of the TOE's logical travel document and used by the inspection system for PACE *Chip Authentication Mapping* of the travel document's chip. It is part of the User Data provided by the TOE for the IT environment.
	PACE *Chip Authentication Mapping* Private Key (SK.CAM)	The PACE *Chip Authentication Mapping* Private Key (SK.CAM) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.
Session keys	CA-K.MAC, CA-K.ENC	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System as result of the Chip Authentication Protocol Version 1.
	PACE-K.MAC, PACE-K.ENC	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) agreed between the TOE and a terminal as result of the PACE Protocol ([ICAO-TR-110]).
Ephemeral keys	ephem-SK.PICC.PACE, ephem-PK.PICC.PACE	The ephemeral PACE Authentication Key Pair {ephem-SK.PICC.PACE, ephem-PK.PICC-PACE} is used for Key Agreement Protocols Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to [BSI-TR-03111-V210-ECC] / [ICAO-TR-110] or DH according to [RSA-PKCS-3-V1.4].

Notes

1. The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as "foreign" in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From travel document's point of view the domestic Document Verifier belongs to the issuing State or Organization.
2. With the optional Active Authentication a key pair is stored in the chip.
3. According to OE.AA_Key_Travel_Document the hash value of ACTIVE AUTHENTICATION PUBLIC KEY INFO (cf. [ICAO-9303-2015] part 11, section 6.1 is stored in the Document Security Object (SO_D) for verifying the key using Passive Authentication.
4. The reference to the ISO 11770-3 which defines ECDH is taken over literally from the table in the protection profile [BSI-CC-PP-0056-V2-2012-MA-02]. All other parts of the ST reference different implementation standards.

7.6 Security Functional Requirements for the TOE

7.6.1 Class FCS Cryptographic support

The iterations of *FCS_CKM.1/CA_EC Cryptographic key generation - EC Diffie-Hellman for Chip Authentication session keys* and *FCS_COP.1/EC (Cryptographic operation – EC)* are caused by different cryptographic (key generation) algorithms to be implemented and keys to be generated by the TOE and shall meet their respective requirements as specified in [CC-Part2-V3.1].

7.6.1.1 FCS_CKM.1/CA_EC Cryptographic key generation - EC Diffie-Hellman for Chip Authentication session keys

EAC

Hierarchical to No other components.

Dependencies

[FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/CA_EC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH**[2] and specified cryptographic key sizes **128, 192, 256 bits (for AES)**[3] that meet the following:

(1) **based on an ECDH protocol compliant to** [BSI-TR-03111-V210-ECC]

using curves

(2) **see section** *Elliptic curves used*.[4]

Notes

1. FCS_CKM.1/CA_EC implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [BSI-TR-03110-1-V220], section 3.1.
2. The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [BSI-TR-03110-1-V220] chapter "3.4 Chip Authentication Version 1". The protocol used by this TOE bases on the Diffie-Hellman-Protocol compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm) (cf. [BSI-TR-03111-V210-ECC], for details). The shared secret value is used to derive the Chip Authentication Session Keys (CA-K.MAC, CA-K.Enc) used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [BSI-TR-03110-1-V220]).
3. The TOE uses the hash functions SHA-1 and SHA-256 of the library SHA (HCL52 v1.12.001) provided by the underlying chip SLC52GDA448* for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms according to [BSI-TR-03110-3-V221] "A.2.3.2. AES".
4. The TOE destroys any session keys in accordance with FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011-MA-01] 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.

[2] [assignment: cryptographic key generation algorithm]
[3] [assignment: cryptographic key sizes]
[4] [selection: based on the Diffie-Hellman key derivation protocol compliant to [BSI-TR-03110-1-V220] and [RSA-PKCS-3-V1.4] , based on an ECDH protocol compliant to [BSI-TR-03111-V210-ECC]]

(iii) The TOE destroys the PACE Session Keys after generation of a Chip Authentication Session Keys and changes the secure messaging to the Chip Authentication Session Keys.

(iv) The TOE clears 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.

Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA_EC.

5. See also FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the key sizes used.
6. See also section *Hash functions implemented*.
7. If PACE *Chip Authentication Mapping* is performed, the Secure Messaging session established by the PACE protocol is sustained. In this case FCS_CKM.1/DH_PACE_EC applies instead of FCS_CKM.1/CA_EC.

7.6.1.2 FCS_CKM.1/CA_RSA Cryptographic key generation - RSA DH for Chip Authentication session keys

EAC

Hierarchical to No other components.

Dependencies

[FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/CA_RSA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **DH**[5] and specified cryptographic key sizes **128, 192, 256 bits (for AES)**[6] that meet the following:

(1) **based on the Diffie-Hellman key derivation protocol compliant to** [RSA-PKCS-3-V1.4] **and** [BSI-TR-03110-1-V220].[7]

Notes

1. FCS_CKM.1/CA_RSA is iterated from FCS_CKM.1/CA_EC.
2. For computing the shared secret the modular exponentation function provided by the RSA crypto library of SLC52GDA448* is used.
3. FCS_CKM.1/CA_RSA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [BSI-TR-03110-1-V220], section 3.1.
4. The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [BSI-TR-03110-1-V220] chapter "3.4 Chip Authentication Version 1". The protocol used by this TOE bases on the Diffie-Hellman-Protocol compliant to [RSA-PKCS-3-V1.4] (i.e. modulo arithmetic based cryptographic algorithm, cf. [RSA-PKCS-3-V1.4]). The shared secret value is used to derive the Chip Authentication Session Keys (CA-K.MAC, CA-K.Enc) used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [BSI-TR-03110-1-V220]).

[5] [assignment: cryptographic key generation algorithm]
[6] [assignment: cryptographic key sizes]
[7] [selection: based on the Diffie-Hellman key derivation protocol compliant to [BSI-TR-03110-1-V220] and [RSA-PKCS-3-V1.4] , based on an ECDH protocol compliant to [BSI-TR-03111-V210-ECC]]

5. The TOE uses the hash functions SHA-1 and SHA-256 of the library SHA (HCL52 v1.12.001) provided by the underlying chip SLC52GDA448* for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms according to [BSI-TR-03110-3-V221] chapter "A.2.3.2. AES".
6. The TOE destroys any session keys in accordance with FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011-MA-01] 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 destroys the PACE Session Keys after generation of a Chip Authentication Session Keys and changes the secure messaging to the Chip Authentication Session Keys.
   (iv) The TOE clears 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.

   Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA_RSA.
7. See also FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the key sizes used.
8. See also section *Hash functions implemented*.
9. If PACE *Chip Authentication Mapping* is performed, the Secure Messaging session established by the PACE protocol is sustained. In this case FCS_CKM.1/DH_PACE_RSA applies instead of FCS_CKM.1/CA_RSA.

7.6.1.3 FCS_CKM.1/DH_PACE_EC Cryptographic key generation - EC Diffie-Hellman for PACE session keys

PACE

Hierarchical to No other components.

Dependencies

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

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

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

FCS_CKM.1.1/DH_PACE_EC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH compliant to** [BSI-TR-03111-V210-ECC][8] and specified cryptographic key sizes **128, 192, 256 bits (for AES)**[9] that meet the following:

(1) [ICAO-TR-110]

using curves

(2) **see section** *Elliptic curves used*.[10]

[8] [selection: Diffie-Hellman-Protocol compliant to [RSA-PKCS-3-V1.4], ECDH compliant to [BSI-TR-03111-V210-ECC]]
[9] [assignment: cryptographic key sizes]
[10] REFINEMENT

Notes

1. See also FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the key sizes used.
2. The TOE generates a shared secret value K with the terminal during the PACE protocol, see [ICAO-TR-110]. The shared secret value K is used for deriving the AES session keys for message encryption and message authentication (PACE-K.MAC, PACE-K.Enc) according to [ICAO-TR-110] for the TSF required by FCS_COP.1/PACE_ENC (see FCS_COP.1/CA_ENC Note 5) and FCS_COP.1/PACE_MAC (see FCS_COP.1/CA_MAC Note 5).
3. FCS_CKM.1/DH_PACE_EC implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [ICAO-TR-110].
4. The TOE destroys any session keys in accordance with FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011-MA-01] after
   (i) detection of an error in a received command by verification of the MAC and
   (ii) The TOE clears 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.
5. See also section *Hash functions implemented*.
6. If a configuration of the TOE uses FCS_CKM.1/DH_PACE_RSA for PACE session key, it must not use this SFR additionally.

7.6.1.4 FCS_CKM.1/DH_PACE_RSA Cryptographic key generation - RSA Diffie-Hellman for PACE session keys

PACE

Hierarchical to No other components.

Dependencies

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

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

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

FCS_CKM.1.1/DH_PACE_RSA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Diffie-Hellman-Protocol compliant to** [RSA-PKCS-3-V1.4][11] and specified cryptographic key sizes **128, 192, 256 bits (for AES)**[12] that meet the following:

(1) [ICAO-TR-110] **(section 3.4.1 Key Agreement Algorithms, table 1)**

using bit lengths

(2) **2048-bit MODP Group (p component) with 224-bit Prime Order Subgroup (q component) or**

(3) **2048-bit MODP Group (p component) with 256-bit Prime Order Subgroup (q component)**[13]

[11] [selection: Diffie-Hellman-Protocol compliant to [RSA-PKCS-3-V1.4], ECDH compliant to [BSI-TR-03111-V210-ECC]]
[12] [assignment: cryptographic key sizes]
[13] REFINEMENT

Notes

1. FCS_CKM.1/DH_PACE_RSA is iterated from FCS_CKM.1/DH_PACE_EC.
2. For computing the shared secret the modular exponentation function of the RSA crypto library provided by SLC52GDA448* is used.
3. See also FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the key sizes used.
4. The TOE generates a shared secret value K with the terminal during the PACE protocol, see [ICAO-TR-110]. The shared secret value K is used for deriving the AES session keys for message encryption and message authentication (PACE-K.MAC, PACE-K.Enc) according to [ICAO-TR-110] for the TSF required by FCS_COP.1/PACE_ENC (see FCS_COP.1/CA_ENC Note 5) and FCS_COP.1/PACE_MAC (see FCS_COP.1/CA_MAC Note 5).
5. FCS_CKM.1/DH_PACE_RSA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [ICAO-TR-110].
6. The TOE destroys any session keys in accordance with FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011-MA-01] after
   (i) detection of an error in a received command by verification of the MAC and
   (ii) The TOE clears 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.
7. See also section *Hash functions implemented*.
8. If a configuration of the TOE uses FCS_CKM.1/DH_PACE_EC for PACE session key, it must not use this SFR additionally.

7.6.1.5 FCS_CKM.1/EC (Cryptographic key generation – EC)

SSCD

Hierarchical to No other components.

Dependencies

[FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/EC The TSF shall generate an <u>SCD/SVD pair</u>[14] in accordance with a specified cryptographic key generation algorithm **Elliptic Curve EC Key Generation**[15] and specified cryptographic key sizes **256, 384, 512, and 521 bits**[16] that meet the following:

ECDSA Key Generation:

(1) **According to the appendix A4.3 in** [ANSI-X9.62] **the cofactor h is not supported.**

(2) **According to section 6.4.2 in** [ISO-IEC-14888-3]

(3) **According to Appendix A.16.9 in** [IEEE-1363]

using curves

(4) **see section** *Elliptic curves used*.[17]

[14] The refinement substitutes "cryptographic keys" by "SCD/SVD pairs" because it clearly addresses the SCD/SVD key generation.
[15] [assignment: cryptographic key generation algorithm]
[16] [assignment: cryptographic key sizes]
[17] [assignment: list of standards]

Notes

1. FCS_CKM.1/EC amounts to requirement "FCS_CKM.1" with the selection of ECC key generation.
2. This TOE uses the crypto libraries RSA v2.08.007, EC v2.08.007, Toolbox v2.08.007, Base v2.08.007, SHA-2 v1.12.001 and Symmetric Crypto Library (SCL) v2.04.002 of the underlying chip SLC52GDA448*.
3. For the cryptographic key generation algorithm "Elliptic Curve EC Key Generation" see [Infineon-ST-SLC52-H13], 7.1.4.5.4 Elliptic Curve (EC) key generation.
4. If a configuration of the TOE uses FCS_CKM.1/RSA, it must not use this SFR additionally.

7.6.1.6 FCS_CKM.1/RSA (Cryptographic key generation – RSA)

SSCD

Hierarchical to No other components.

Dependencies

[FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/RSA The TSF shall generate an SCD/SVD pair[18] in accordance with a specified cryptographic key generation algorithm **RSA key generation**[19] and specified cryptographic key sizes **2048, 3072, and 4096 bits**[20] that meet the following:

(1) [RSA-PKCS1-v2.2], **sections 3.1 and 3.2 for u=2, i.e., without any** (r_i, d_i, t_i), **i > 2.**:

- **public key representation 3.1 supported for n <** $2^{4096 + 128}$,
- **private key representation 3.2(1) supported for n <** $2^{2048 + 64}$,
- **private key representation 3.2(2) supported for p × q <** $2^{4096 + 128}$

(2) **and** [IEEE-1363], **section 8.1.3.1**:

- **public key representation 8.1.3.1(1) supported for n <** $2^{2048 + 64}$,
- **private key representation 8.1.3.1(2) supported for p × q <** $2^{4096 + 128}$,
- **private key representation 8.1.3.1(3) supported for p × q <** $2^{2048 + 64}$[21]

Notes

1. FCS_CKM.1/RSA is added to contents of PP [BSI-CC-PP-0059-2009-MA-02] (iterated).
2. This TOE uses the crypto libraries RSA v2.08.007, EC v2.08.007, Toolbox v2.08.007, Base v2.08.007, SHA-2 v1.12.001 and Symmetric Crypto Library (SCL) v2.04.002 of the underlying chip SLC52GDA448*.

[18] The refinement substitutes "cryptographic keys" by "SCD/SVD pairs" because it clearly addresses the SCD/SVD key generation.
[19] [assignment: cryptographic key generation algorithm]
[20] [assignment: cryptographic key sizes]
[21] [assignment: list of standards]

3. For the cryptographic key generation algorithm "RSA Key Generation" see [Infineon-ST-SLC52-H13] 7.1.4.5 Rivest-Shamir-Adleman (RSA) key generation.
4. The standard PKCS #1 version 2.2 [RSA-PKCS1-v2.2] supersedes the standard PKCS #1 version 2.1, which is referenced in the [Infineon-ST-SLC52-H13]. However, version 2.2 only includes compatible techniques; both versions are equivalent in this context.
5. If a configuration of the TOE uses FCS_CKM.1/EC, it must not use this SFR additionally.

7.6.1.7 FCS_CKM.4 Cryptographic key destruction

Hierarchical to No other components.

Dependencies

[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting with zeros**[22] that meets the following: **none**[23].

Notes

1. The TOE shall destroy the PACE / CA 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.
2. The cryptographic key SCD will be destroyed on demand of the signatory. The signatory may want to destruct the SCD stored in the SSCD e.g. after the qualified certificate for the corresponding SVD is not valid anymore.
3. The personalization key will be destroyed after the end of the personalization.

7.6.1.8 FCS_COP.1/EC (Cryptographic operation – EC)

SSCD

Hierarchical to No other components.

Dependencies

[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/EC The TSF shall perform digital signature creation[24] in accordance with a specified cryptographic algorithm **Elliptic Curve Digital Signature Algorithm (ECDSA)**[25] and cryptographic key sizes **256, 384, 512, and 521 bits**[26] that meet the following:

Signature Generation:

1. **According to section 7.3 in** [ANSI-X9.62].

[22] [assignment: cryptographic key destruction method]
[23] [assignment: list of standards]
[24] [assignment: list of cryptographic operations]
[25] [assignment: cryptographic algorithm]
[26] [assignment: cryptographic key sizes]

- **Step d) and e) not supported.**
- **The output of step e) has to be provided as input to our function by the caller.**
- **Deviation of step c) and f):**
  - **The jumps to step a) were substituted by a return of the function with an error code, the jumps are emulated by another call to our function.**

2. **According to section 6.4.3 in** [ISO-IEC-14888-3].
   - **6.4.3.3 not supported.**
   - **6.4.3.5 not supported:**
     - **The hash-code H of the message has to be provided by the caller as input to our function.**
   - **6.4.3.7 not supported.**
   - **6.4.3.8 not supported.**
3. **According to section 7.2.7 in** [IEEE-1363]:
   - **Deviation of step (3) and (4):**
     - **The jump to step 1, were substituted by a return of the function with an error code, the jumps are emulated by another call to our function.**

using curves

4. **see section** *Elliptic curves used*.[27]

Notes

1. FCS_COP.1/EC amounts to requirement "FCS_COP.1" with the selection of ECDSA.
2. This TOE uses the crypto libraries RSA v2.08.007, EC v2.08.007, Toolbox v2.08.007, Base v2.08.007, SHA-2 v1.12.001 and Symmetric Crypto Library (SCL) v2.04.002 of the underlying chip SLC52GDA448*.
3. For the Elliptic Curve Digital Signature Algorithm (ECDSA) see [Infineon-ST-SLC52-H13], "7.1.4.6.4 Elliptic Curve DSA (ECDSA) operation", section "Signature Generation and Verification".
4. If a configuration of the TOE uses FCS_COP.1/RSA, it must not use this SFR additionally.

7.6.1.9 FCS_COP.1/RSA (Cryptographic operation – RSA)

SSCD

Hierarchical to No other components.

Dependencies

[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/RSA The TSF shall perform digital signature creation[28] in accordance with a specified cryptographic algorithm **Rivest-Shamir-Adleman**

[27] [assignment: list of standards]
[28] [assignment: list of cryptographic operations]

(RSA)[29] and cryptographic key sizes **2048, 3072, and 4096 bits**[30] that meet the following:

Signature Generation (with or without CRT):

1. **According to section 5.2.1 RSASP1 in** [RSA-PKCS1-v2.2], **for u=2, i.e., without any** (r_i, d_i, t_i), **i > 2**:
   - **5.2.1(1) not supported,**
   - **5.2.1(2.a) supported for n <** $2^{2048 + 64}$,
   - **5.2.1(2b) supported for p x q <** $2^{4096 + 128}$,
   - **5.2.1(2b) (ii)&(v) not applicable due to u = 2**
2. **According to section 8.2.4 in** [IEEE-1363]:
   - **8.2.1(I) supported for n <** $2^{2048 + 64}$,
   - **8.2.1(II) supported for p x q <** $2^{4096 + 128}$
   - **8.2.1(III) not supported.**[31]

Notes

1. FCS_COP.1/RSA is added to contents of PP [BSI-CC-PP-0059-2009-MA-02] (iterated).
2. This TOE uses the crypto libraries RSA v2.08.007, EC v2.08.007, Base v2.08.007, SHA-2 v1.12.001 and Symmetric Crypto Library (SCL) v2.04.002 of the underlying chip SLC52GDA448*.
3. For the "Rivest-Shamir-Adleman (RSA)" see [Infineon-ST-SLC52-H13], "7.1.4.6.1 Rivest-Shamir-Adleman (RSA) operation".
4. The standard PKCS #1 version 2.2 [RSA-PKCS1-v2.2] supersedes the standard PKCS #1 version 2.1, which is referenced in the [Infineon-ST-SLC52-H13]. However, version 2.2 only includes compatible techniques; both versions are equivalent in this context.
5. The padding is done according to RSASSA-PSS and RSASSA-PKCS1-v1_5.
6. If a configuration of the TOE uses FCS_COP.1/EC, it must not use this SFR additionally.

7.6.1.10 FCS_COP.1/SHA (Cryptographic operation – Hash calculation)

SSCD

Hierarchical to No other components.

Dependencies

[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

fulfilled by 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.
- a respective key destruction cannot be expected here.

[29] [assignment: cryptographic algorithm]
[30] [assignment: cryptographic key sizes]
[31] [assignment: list of standards]

FCS_COP.1.1/SHA The TSF shall perform **hash-value calculation of user chosen data**[32] in accordance with a specified cryptographic algorithm **SHA-1, SHA-256, SHA-384 and SHA-512**[33] and cryptographic key sizes **none**[34] that meet the following:

[NIST-FIPS-180-4] **with chapters 6.1 "SHA-1", 6.2 "SHA-256", 6.4 "SHA-512" and 6.5 "SHA-384".**[35]

Notes

1. FCS_COP.1/SHA is added to contents of PP [BSI-CC-PP-0059-2009-MA-02] (not iterated).
2. This TOE uses the SHA library (HCL52 v1.12.001) of the underlying chip SLC52GDA448*.
3. The requirements for the hashing functions used for PACE are included in SFRs *FCS_CKM.1/DH_PACE_EC* and *FCS_CKM.1/DH_PACE_RSA*.
4. FCS_COP.1/SHA is used for internally calculated hash values which are used afterward for the signature creation including last round hash values.

7.6.1.11 FCS_COP.1/AES_MAC (Cryptographic operation – MACing with AES)

SSCD

Hierarchical to No other components.

Dependencies

[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4 is fulfilled. FCS_ITC.1/2 is not fulfilled, but **justified**: The key used here is managed in a similar way as other initialization data in the sense that it is imported during manufacturing (FMT_MTD.1/INI_ENA) and used only during personalisation and made unavailable afterwards ((FMT_MTD.1/INI_DIS). Therefore, no dedicated import policy is needed.

FCS_COP.1.1/AES_MAC The TSF shall perform **message authentication code in CMAC**[36] in accordance with a specified cryptographic algorithm **Advanced Encryption Standard (AES) in CMAC mode**[37] and cryptographic key sizes **192 bit**[38] that meet the following: [NIST-FIPS-197] **and** [ISO-IEC-9797-1-2011][39].

Notes

1. FCS_COP.1/AES_MAC is added to contents of [BSI-CC-PP-0059-2009-MA-02] (not iterated).
2. This SFR covers the cryptographic operation used during the Symmetric Authentication Mechanism with the Administrator Personalization Key. This key is imported by the administrator during the TOE initialization and is used to secure the TOE personalization.

---

[32] [assignment: list of cryptographic operations]
[33] [assignment: cryptographic algorithm]
[34] [assignment: cryptographic key sizes]
[35] [assignment: list of standards]
[36] [assignment: list of cryptographic operations]
[37] [assignment: cryptographic algorithm]
[38] [assignment: cryptographic key sizes]
[39] [assignment: list of standards]

7.6.1.12 FCS_COP.1/CA_ENC (Cryptographic operation - Symmetric Encryption / Decryption)

EAC

Hierarchical to No other components.

Dependencies

[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

fulfilled by

- FCS_CKM.1/DH_PACE_EC
- FCS_CKM.1/DH_PACE_RSA
- FCS_CKM.4.1

FCS_COP.1.1/CA_ENC The TSF shall perform secure messaging - encryption and decryption[40] in accordance with a specified cryptographic algorithm **AES in CBC mode**[41] and cryptographic key sizes **using AES with 128, 192, 256 bits**[42] that meet the following:

(1) **(for CBC:)** [NIST-800-38A-2001], **chapter 6.2 THE CIPHER BLOCK CHAINING MODE.**

(2) **(for AES:) U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), FIPS PUB 197**.[43]

Notes

1. This TOE uses the Symmetric Crypto Library (SCL52 v2.04.002) provided by the underlying chip SLC52GDA448*.
2. This TOE uses the AES provided by the underlying chip SLC52GDA448*.
3. For the "Advanced Encryption Standard (AES)" see [Infineon-ST-SLC52-H13], 7.1.4.2.2 AES Operation.
4. This SFR requires the TOE to implement the cryptographic primitives (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_EC (and FCS_CKM.1/CA_RSA).

[40] [assignment: list of cryptographic operations]
[41] [assignment: cryptographic algorithm]
[42] [assignment: cryptographic key sizes]
[43] [assignment: list of standards]

7.6.1.13 FCS_COP.1/CA_MAC (Cryptographic operation - MAC)

EAC

Hierarchical to No other components.

Dependencies

[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/CA_MAC The TSF shall perform secure messaging - message authentication code[44] in accordance with a specified cryptographic algorithm **CMAC**[45] and cryptographic key sizes **using AES with 128, 192, 256 bits**[46] that meet the following:

(1) **(for CMAC:)** [ISO-IEC-9797-1-2011], **algorithm 5 and padding method 2**.

(2) **(for AES:) U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL), Advanced Encryption Standard (AES),** [NIST-FIPS-197].[47]

Notes

1. This TOE uses the Symmetric Crypto Library (SCL52 v2.04.002) provided by the underlying chip SLC52GDA448*.
2. This TOE uses the AES provided by the underlying chip SLC52GDA448*.
3. For the "Advanced Encryption Standard (AES)" see [Infineon-ST-SLC52-H13], 7.1.4.2.2 AES Operation.
4. 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 PACE Protocol according to the FCS_CKM.1/DH_PACE_EC and FCS_CKM.1/DH_PACE_RSA. Furthermore the SFR is used for authentication attempts of a terminal as Personalization Agent by means of the authentication mechanism.

7.6.1.14 FCS_COP.1/PACE_ENC (Cryptographic operation - Encryption / Decryption AES)

PACE

Hierarchical to No other components.

Dependencies

[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

fulfilled by

- FCS_CKM.1/DH_PACE_EC **and** FCS_CKM.1/DH_PACE_RSA
- FCS_CKM.4

[44] [assignment: list of cryptographic operations]
[45] [assignment: cryptographic algorithm]
[46] [assignment: cryptographic key sizes]
[47] [assignment: list of standards]

FCS_COP.1.1/PACE_ENC The TSF shall perform secure messaging - encryption and decryption[48] in accordance with a specified cryptographic algorithm **AES in CBC mode**[49] and cryptographic key sizes **128, 192, 256 (for AES)**[50] bit that meet the following:

compliant to [ICAO-TR-110][51].

Note

1. This TOE uses the Symmetric Crypto Library (SCL52 v2.04.002) provided by the underlying chip SLC52GDA448*.
2. This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE_EC (PACE-K.Enc) and FCS_CKM.1/DH_PACE_RSA.

7.6.1.15 FCS_COP.1/PACE_MAC (Cryptographic operation - MAC)

PACE

Hierarchical to No other components.

Dependencies

[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

fulfilled by

- FCS_CKM.1/DH_PACE_EC **and** FCS_CKM.1/DH_PACE_RSA
- FCS_CKM.4

FCS_COP.1.1/PACE_MAC The TSF shall perform secure messaging - message authentication code[52] in accordance with a specified cryptographic algorithm **(AES) CMAC**[53] and cryptographic key sizes **128, 192, 256 (for AES)**[54] bit that meet the following:

compliant to [ICAO-TR-110][55].

Notes

1. This TOE uses the Symmetric Crypto Library (SCL52 v2.04.002) provided by the underlying chip SLC52GDA448*.
2. This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE_EC (PACE-K.MAC) and FCS_CKM.1/DH_PACE_RSA.

---

48 [assignment: list of cryptographic operations]
49 [assignment: cryptographic algorithm]
50 [assignment: cryptographic key sizes]
51 [assignment: list of standards]
52 [assignment: list of cryptographic operations]
53 [assignment: cryptographic algorithm]
54 [assignment: cryptographic key sizes]
55 [assignment: list of standards]

7.6.1.16 FCS_COP.1/SIG_VER_EC (Cryptographic operation - Signature verification by travel document with EC)

EAC

Hierarchical to No other components.

Dependencies

[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SIG_VER_EC The TSF shall perform digital signature verification[56] in accordance with a specified cryptographic algorithm **ECDSA**[57] and cryptographic key sizes **256, 384, 512, and 521 bits**[58] that meet the following:

(1) **According to section 7.4.1 in** [ANSI-X9.62] **Not implemented is step b) and c) thereof. The output of step c) has to be provided as input to our function by the caller. Deviation of step d): Beside noted calculation, our algorithm adds a random multiple of BasepointerOrder n to the calculated values u1 and u2.**

(2) **According to sections 6.4.4 in** [ISO-IEC-14888-3]. **Not supported are sections 6.4.4.2 and 6.4.4.3: The hash-code H of the message has to be provided by the caller as input to the function.**

(3) **According to section 7.2.8 ECVP-DSA in** [IEEE-1363].

using curves

(4) **see section** *Elliptic curves used*.[59]

Notes

1. Due to the fact that there is a SFR added to this ST using RSA for signature verification the SFR "FCS_COP.1/SIG_VER" of [BSI-CC-PP-0056-V2-2012-MA-02] is renamed to "FCS_COP.1/SIG_VER_EC" for mnemonic reason.
2. This TOE uses the ECDSA (Signature Verification) provided by the underlying chip SLC52GDA448*.
3. The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.
4. The TOE implements ECDSA (and RSA cf. FCS_COP.1/SIG_VER_RSA) for the Terminal Authentication Protocol v.1 (cf. [BSI-TR-03110-3-V221] A.6.4.Terminal Authentication with ECDSA).
5. See also section *Hash functions implemented*.
6. If a configuration of the TOE uses FCS_COP.1/SIG_VER_RSA, it must not use this SFR additionally.

---

[56] [assignment: list of cryptographic operations]
[57] [assignment: cryptographic algorithm]
[58] [assignment: cryptographic key sizes]
[59] [assignment: list of standards]

7.6.1.17 FCS_COP.1/SIG_VER_RSA (Cryptographic operation - Signature verification by travel document with RSA)

EAC

Hierarchical to No other components.

Dependencies

[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SIG_VER_RSA The TSF shall perform digital signature verification[60] in accordance with a specified cryptographic algorithm **RSA**[61] and cryptographic key sizes **2048 and 3072 bits**[62] (cf. [BSI-TR-03110-3-V221] section A.7.3.2.Public Key Format) that meet the following:

(1) **According to section 5.2.2 RSAVP1 in** [RSA-PKCS1-v2.2]

(2) **Padding according to RSASSA-PSS or**

(3) **Padding according to RSASSA-PKCS1-v1_5**.[63]

Notes

1. SFR FCS_COP.1/SIG_VER_RSA is iterated from PP SFR FCS_COP.1/SIG_VER_EC ("FCS_COP.1/SIG_VER").
2. This TOE uses the RSA (Signature Verification) provided by the underlying chip SLC52GDA448*.
3. For the "digital signature verification" see [Infineon-ST-SLC52-H13], 7.1.4.6.1 Rivest-Shamir-Adleman (RSA) operation, section "Signature Verification:".
4. The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge
5. See also section *Hash functions implemented*.
6. The bit lengths for TA are taken over from [BSI-TR-03110-3-V221] section A.7.3.2. Public Key Format.
7. The TOE implements RSA (and ECDSA cf. FCS_COP.1/SIG_VER_EC) for the Terminal Authentication Protocol v.1 (cf. [BSI-TR-03110-3-V221] section A.6.3.Terminal Authentication with RSA).
8. If a configuration of the TOE uses FCS_COP.1/SIG_VER_EC, it must not use this SFR additionally.

---

[60] [assignment: list of cryptographic operations]
[61] [assignment: cryptographic algorithm]
[62] [assignment: cryptographic key sizes]
[63] [assignment: list of standards]

7.6.1.18 FCS_COP.1/AA_SGEN_EC (Cryptographic operation - Signature generation for AA with EC)

EAC

Hierarchical to No other components.

Dependencies

[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/AA_SGEN_EC The TSF shall perform **digital signature generation**[64] in accordance with a specified cryptographic algorithm **ECDSA**[65] and cryptographic key sizes **256, 384, 512, and 521 bits**[66] that meet the following:

Signature Generation:

1. **According to section 7.3 in** [ANSI-X9.62].
   - **Step d) and e) not supported.**
   - **The output of step e) has to be provided as input to our function by the caller.**
   - **Deviation of step c) and f):**
     - **The jumps to step a) were substituted by a return of the function with an error code, the jumps are emulated by another call to our function.**
2. **According to section 6.4.3 in** [ISO-IEC-14888-3].
   - **6.4.3.3 not supported.**
   - **6.4.3.5 not supported:**
     - **The hash-code H of the message has to be provided by the caller as input to our function.**
   - **6.4.3.7 not supported.**
   - **6.4.3.8 not supported.**
3. **According to section 7.2.7 in** [IEEE-1363]:
   - **Deviation of step (3) and (4):**
     - **The jump to step 1, were substituted by a return of the function with an error code, the jumps are emulated by another call to our function.**

using curves

4. **see section** *Elliptic curves used*.[67]

Notes

1. SFR FCS_COP.1/AA_SGEN_EC is added to contents of PPs [BSI-CC-PP-0056-V2-2012-MA-02] and [BSI-CC-PP-0068-V2-2011-MA-01].
2. See also section *Hash functions implemented*.

64 [assignment: list of cryptographic operations]
65 [assignment: cryptographic algorithm]
66 [assignment: cryptographic key sizes]
67 [assignment: list of standards]

3. The signature generation is used to perform Active Authentication.
4. The TOE implements ECDSA and RSA (cf. FCS_COP.1/AA_SGEN_RSA) for the Active Authentication Protocol (cf. [BSI-TR-03110-3-V221] section 1.2 Active Authentication).
5. If a configuration of the TOE uses FCS_COP.1/AA_SGEN_RSA, it must not use this SFR additionally.

7.6.1.19 FCS_COP.1/AA_SGEN_RSA (Cryptographic operation - Signature generation for AA with RSA)

EAC

Hierarchical to No other components.

Dependencies

[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/AA_SGEN_RSA The TSF shall perform **digital signature generation**[68] in accordance with a specified cryptographic algorithm **RSA**[69] and cryptographic key sizes **2048, 3072, and 4096 bits**[70] that meet the following:

(1) **Signature Generation (with or without CRT): According to section 5.2.1 RSASP1 in [RSA-PKCS1-v2.2] for u = 2, i.e., without any (r_i, d_i, t_i), i >2, therefore without 5.2.1.2.b (ii)&(v), without 5.2.1.1. 5.2.1.2.a.**

(2) **Padding according ISO/IEC 9796-2 Digital Signature scheme 1 according to [ICAO-9303-2015] part 11, section "6.1 Active Authentication".**[71]

Notes

1. SFR FCS_COP.1/AA_SGEN_RSA is iterated from SFR FCS_COP.1/AA_SGEN_EC.
2. This TOE uses the RSA (Signature Generation) provided by the underlying chip SLC52GDA448*.
3. For the "digital signature generation" see [Infineon-ST-SLC52-H13], 7.1.4.6.1 Rivest-Shamir-Adleman (RSA) operation, section "Signature Generation (with or without CRT):".
4. See also section *Hash functions implemented*.
5. The signature generation is used to perform Active Authentication.
6. The TOE implements RSA and ECDSA (cf. FCS_COP.1/AA_SGEN_EC) for the Active Authentication Protocol (cf. [BSI-TR-03110-3-V221] section 1.2 Active Authentication).
7. If a configuration of the TOE uses FCS_COP.1/AA_SGEN_EC, it must not use this SFR additionally.

---

[68] [assignment: list of cryptographic operations]
[69] [assignment: cryptographic algorithm]
[70] [assignment: cryptographic key sizes]
[71] [assignment: list of standards]

7.6.1.20 FCS_RNG.1 (Random number generation)

Hierarchical to No other components.

Dependencies No dependencies.

FCS_RNG.1.1 The TSF shall provide a **hybrid deterministic**[72] random number generator that implements:

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

(DRG.4.2) The RNG provides forward secrecy.

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

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

(DRG.4.5) The internal state of the RNG is seeded by a PTRNG of class PTG.2 according to [BSI-AIS31-V3].[73]

FCS_RNG.1.2 The TSF shall provide **random numbers** that meet:

(DRG.4.6) The RNG generates output for which 2^{12} **strings of bit length 128 are mutually different with probability** $1\text{-}2^{-105}$ **(acc. to** [NIST-SP800-90A] **C.3).**

(DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A as defined in [BSI-AIS2031-RNG-CLASSES-V2].[74]

Notes

1. This SFR has been adapted from [BSI-CC-PP-0084-2014] (FCS_RNG.1) to meet [BSI-AIS2031-RNG-CLASSES-V2]. It correlates with the SFR 'FCS_RND.1' from [BSI-CC-PP-0068-V2-2011-MA-01].
2. For the "random numbers generation Class PTG.2 according to [BSI-AIS31-V3]" see [Infineon-ST-SLC52-H13] "7.1.1.1.1 True Random Number Generation".
3. Entropy source uses PTG.2 of the hardware as noise source and Block_Cipher_df as specified in [NIST-SP800-90A] using the AES block cipher as a conditioning component to implement CTR_DRBG as specified in [NIST-SP800-90A].
4. This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocol (PACE) as required by FIA_UAU.4/PACE (1).
5. This SFR requires the TOE to generate random numbers (random nonce) used also for Terminal Authentication Protocol v.1 as required by FIA_UAU.4/PACE (3).

---

[72] [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]
[73] [assignment: list of security capabilities]
[74] [assignment: a defined quality metric]

7.6.2 Class FIA Identification and Authentication

Table 7.5 provides an overview on the authentication mechanisms used

Table 7.5: Overview on authentication SFR

Name	SFR for the TOE
Authentication Mechanism for Personalization Agents	FIA_UAU.4/PACE
Chip Authentication Protocol v.1	FIA_API.1/CA FIA_UAU.5/PACE FIA_UAU.6/EAC
Active Authentication Protocol	FIA_UAU.5/PACE FIA_API.1/AA
Terminal Authentication Protocol v.1	FIA_UAU.5/PACE
PACE protocol[77]	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_UAU.6/PACE[78] FIA_AFL.1/PACE
Passive Authentication	FIA_UAU.5/PACE

Note the Chip Authentication Protocol Version 1 as used by this TOE includes

- the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol Version 1,
- the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

The Chip Authentication Protocol v.1 may be used independent of the Terminal Authentication Protocol v.1. But if the Terminal Authentication Protocol v.1 is used the terminal shall use the same public key as presented during the Chip Authentication Protocol v.1.

If PACE *Chip Authentication Mapping* is used,the secure messaging keys established by the PACE protocol are sustained. A subsequent Terminal Authentication Protocol v.1 uses the PACE-CAM public key verified during the PACE protocol.

7.6.2.1 FIA_UID.1/PACE (Timing of identification)

PACE
EAC

Hierarchical to No other components.

Dependencies No dependencies.

FIA_UID.1.1/PACE The TSF shall allow

1. to establish the communication channel
2. carrying out the PACE Protocol according to [ICAO-TR-110]
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
4. to carry out the Chip Authentication Protocol v.1 according to [BSI-TR-03110-1-V220]
5. to carry out the Terminal Authentication Protocol v.1 according to [BSI-TR-03110-1-V220][79]
6. **to carry out the Active Authentication Protocol according to** [ICAO-TR-110]
7. **to carry out the PACE *Chip Authentication Mapping* protocol according to** [ICAO-TR-110]

[77] Only listed for information purposes
[78] not listed in PP [BSI-CC-PP-0056-V2-2012-MA-02]
[79] [assignment: list of TSF-mediated actions]

8. **to run self tests according to** FPT_TST.1[80]

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

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

Notes

1. The SFR FIA_UID.1/PACE in the current ST covers the definition in PACE PP [BSI-CC-PP-0068-V2-2011-MA-01] and extends it by EAC aspect 4. This extension does not conflict with the strict conformance to PACE PP.
2. In the Phase 2 "Manufacturing of the TOE" 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 travel document manufacturer may create the user role Personalisation Agent for transition from Phase 2 to Phase 3 "Personalisation of the travel 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) Extended Inspection System 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).
3. 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 travel document holder itself or an authorised other person or device (Basic Inspection System with PACE).
4. 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 travel 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).
5. See FIA_AFL.1/PACE how skimming is prevented by the TOE.
6. The notes above stem from the protection profile which uses the generic terminology of [BSI-CC-PP-0084-2014]. For a mapping of the concrete TOE life-cycle to the generic model refer to section *Life Cycle Phases Mapping*.

---

80 [assignment: list of TSF-mediated actions]

7.6.2.2 FIA_UID.1 (Timing of identification)

SSCD

Hierarchical to No other components.

Dependencies No dependencies.

FIA_UID.1.1 The TSF shall allow:

1. self-test according to FPT_TST.1;[81]
2. **carrying out the PACE protocol according to** [ICAO-TR-110]
3. **performing of the Symmetric Authentication Mechanism**[82]

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

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

Notes

1. This SFR has been amended with item (2) from [BSI-CC-PP-0068-V2-2011-MA-01] and with (3) for authenticating the administrator before TOE personalization.
2. User identified after a successfully performed PACE protocol is a PACE authenticated PACE Terminal. Please note that CAN does not effectively represent a secret (but other PACE passwords do so), but is restricted-revealable; i.e. it is either the legitimate user itself or an authorized other person or device (PACE Terminal).
3. After successful PACE authentication using the PIN.ADMIN R.Admin or the IT entity (CGA or SSCD Issuing Application) on its behalf is identified.

7.6.2.3 FIA_UAU.1/PACE (Timing of authentication)

PACE
EAC

Hierarchical to No other components.

Dependencies FIA_UID.1 Timing of identification.

FIA_UAU.1.1/PACE The TSF shall allow

1. to establish the communication channel,
2. carrying out the PACE Protocol according to [ICAO-TR-110][83],
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
4. to identify themselves by selection of the authentication key
5. to carry out the Chip Authentication Protocol Version 1 according to [BSI-TR-03110-1-V220]
6. to carry out the Terminal Authentication Protocol Version 1 according to [BSI-TR-03110-1-V220][84]
7. **to carry out the Active Authentication Protocol according to** [ICAO-TR-110]
8. **to carry out the PACE *Chip Authentication Mapping* protocol according to** [ICAO-TR-110]

---

[81] [assignment: list of TSF mediated actions]
[82] [assignment: list of additional TSF mediated actions]
[83] travel document identifies itself within the PACE protocol by selection of the authentication key ephem-PK.PICC-PACE
[84] [assignment: list of TSF-mediated actions]

9. **to run self tests according to** FPT_TST.1[85]

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

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

Notes

1. The SFR FIA_UID.1/PACE in the current ST covers the definition in PACE PP [BSI-CC-PP-0068-V2-2011-MA-01] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to PACE PP.
2. The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorized other person or device (BIS-PACE). If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-K.MAC, PACE-K.Enc), cf. FTP_ITC.1/PACE.
3. See FIA_AFL.1/PACE how skimming is prevented by the TOE.

7.6.2.4 FIA_UAU.1 (Timing of authentication)

SSCD

Hierarchical to No other components.

Dependencies FIA_UID.1 Timing of identification.

FIA_UAU.1.1 The TSF shall allow:

1. self-test according to FPT_TST.1;
2. identification of the user by means of TSF required by FIA_UID.1;[86]
3. establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD, CGA
4. establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD, SCA
5. **carrying out the PACE protocol according to** [ICAO-TR-110]
6. **performing of the Symmetric Authentication Mechanism**[87]

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

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

Notes

1. This SFR has been amended with item (5) from [BSI-CC-PP-0068-V2-2011-MA-01] and with item (6) for authenticating the administrator before TOE personalization.
2. Item (3) of this SFR only applies for the Life Cycle Phase "Usage/Operational" as the TOE provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase "Usage/Operational".

[85] [assignment: list of TSF-mediated actions]
[86] [assignment: list of TSF mediated actions]
[87] [assignment: list of additional TSF mediated actions]

3. The user authenticated after a successfully performed PACE protocol is a PACE authenticated PACE Terminal. Please note that CAN does not effectively represent a secret (but other PACE passwords do so), but are restricted-revealable; i.e. it is either the legitimate user itself or an authorized other person or device (PACE Terminal).
4. After successful PACE authentication using the PIN.ADMIN R.Admin or the IT entity (CGA or SSCD Issuing Application) on its behalf is authenticated.

7.6.2.5 FIA_UAU.4/PACE (Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE)

PACE
EAC

Hierarchical to No other components.

Dependencies No dependencies

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

1. PACE Protocol according to [ICAO-TR-110]
2. Authentication Mechanism based on **AES**[88]
3. Terminal Authentication Protocol v.1 according to [BSI-TR-03110-1-V220].[89]

Notes

1. The SFR FIA_UAU.4.1/PACE in the current ST covers the definition in PACE PP [BSI-CC-PP-0068-V2-2011-MA-01] and extends it by the EAC aspect 3. This extension does not conflict with the strict conformance to PACE PP. The generation of random numbers (random nonce) used for the authentication protocol (PACE) and Terminal Authentication as required by FIA_UAU.4/PACE is required by FCS_RNG.1 from [BSI-CC-PP-0068-V2-2011-MA-01].
2. The authentication mechanisms uses a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt.
3. Authentication data related to PACE Protocol according to [ICAO-TR-110] include authentication data related to PACE *Chip Authentication Mapping*.

7.6.2.6 FIA_UAU.5/PACE (Multiple authentication mechanisms)

PACE
EAC

Hierarchical to No other components.

Dependencies No dependencies.

FIA_UAU.5.1/PACE The TSF shall provide

1. PACE Protocol according to [ICAO-TR-110]
2. Passive Authentication according to [ICAO-9303-2015], part 11, section 5.1
3. Secure messaging in MAC-ENC mode according to [ICAO-TR-110]
4. Symmetric Authentication Mechanism based on **AES**[90]

[88] [selection: Triple- DES, AES or other approved algorithms]
[89] [assignment: identified authentication mechanism(s)]
[90] [selection: Triple-DES, AES or other approved algorithms]

5. Terminal Authentication Protocol v.1 according to [BSI-TR-03110-1-V220][91]
6. **Active Authentication according to** [ICAO-9303-2015], part 11 section 6.1[92]

to support user authentication.

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

1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.
2. The TOE accepts the authentication attempt as Personalization Agent by **the Authentication Mechanism with Personalization Agent Key(s)**[93].
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.[94]
5. **If PACE *Chip Authentication Mapping* has been performed instead of Chip Authentication Protocol Version 1 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 PACE *Chip Authentication Mapping* and the secure messaging established by the PACE Protocol.**[95]

Notes

1. The SFR FIA_UAU.5.1/PACE in the current ST covers the definition in PACE PP [BSI-CC-PP-0068-V2-2011-MA-01] and extends it by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE in the current ST covers the definition in PACE PP [BSI-CC-PP-0068-V2-2011-MA-01] and extends it by EAC aspects 2), 3), 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.
2. The Active Authentication has been added to the authentication mechanisms to cover it additionally in the evaluation. Adding new mechanisms does not impact the security claims of the Protection Profile.

[91] [assignment: list of multiple authentication mechanisms]
[92] REFINEMENT
[93] [selection: the Authentication Mechanism with Personalization Agent Key(s)]
[94] [assignment: rules describing how the multiple authentication mechanisms provide authentication]
[95] [assignment: rules describing how the multiple authentication mechanisms provide authentication]

7.6.2.7 FIA_UAU.6/EAC (Re-authenticating - Re-authenticating of Terminal by the TOE)

EAC

Hierarchical to No other components.

Dependencies No dependencies.

FIA_UAU.6.1/EAC 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.[96]

Note

1. The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [ICAO-9303-2015], part 11, section 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 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.

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

PACE

Hierarchical to No other components.

Dependencies No dependencies.

FIA_UAU.6.1/PACE The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal.[97]

Notes

1. This SFR has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01].
2. The PACE protocol specified in [ICAO-TR-110] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then authenticate mode based on CMAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.
3. The SFR FIA_UAU.6/PACE also includes PACE *Chip Authentication Mapping*.

---

[96] [assignment: list of conditions under which re-authentication is required]
[97] [assignment: list of conditions under which re-authentication is required]

7.6.2.9 FIA_UAU.6/CA (Re-authenticating – Re-authenticating of Terminal by the TOE)

CGA
SCA

Hierarchical to No other components.

Dependencies No dependencies.

FIA_UAU.6.1/CA 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[98] **or the R.Admin or the IT entity (CGA or SSCD Issuing Application) on its behalf.**[99]

Notes

1. This SFR has been adapted from the SFR FIA_UAU.6/EAC of [BSI-CC-PP-0056-V2-2012-MA-02].
2. The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [ICAO-9303-2015] include secure messaging for all commands exchanged after successful authentication of R.Admin or the IT entity (CGA or SSCD Issuing Application) on its behalf. 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 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.

7.6.2.10 FIA_UAU.6/Signature_Creation (Re-authenticating for Signature Creation)

Hierarchical to No other components.

Dependencies No dependencies.

FIA_UAU.6.1/Signature_Creation The TSF shall re-authenticate the user under the conditions

1. **Single signature S.Sigy before every single DTBS/R signature.**
2. **Limited Mass signature S.Sigy before next signature after card reset or after Application QES was left or otherwise before (N+1)-th DTBS/R signature in a row when limit for consecutive signatures is N.**
3. **Unlimited Mass signature S.Sigy before next signature after card reset or after Application QES was left**[100].

Note

1. This SFR has been added to contents of PP [BSI-CC-PP-0059-2009-MA-02] (not iterated).

---

[98] [assignment: list of conditions under which re-authentication is required]
[99] REFINEMENT, see associated note 2
[100] [assignment: list of conditions under which re-authentication is required]

7.6.2.11 FIA_API.1/CA (Authentication Proof of Identity by Chip Authentication)

EAC

Hierarchical to No other components.

Dependencies No dependencies.

FIA_API.1.1/CA The TSF shall provide a Chip Authentication Protocol Version 1 according to [BSI-TR-03110-1-V220][101] to prove the identity of the TOE[102].

Note

1. Due to the fact that there is a SFR added to this ST using AA for Authentication Proof of Identity the SFR "FIA_API.1" of [BSI-CC-PP-0056-V2-2012-MA-02] is renamed to "FIA_API.1/CA" for mnemonic reason.
2. This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [BSI-TR-03110-1-V220]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [ICAO-9303-2015].

   The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

7.6.2.12 FIA_API.1/AA (Authentication Proof of Identity by Active Authentication)

Hierarchical to No other components.

Dependencies No dependencies.

FIA_API.1.1/AA The TSF shall provide a **Active Authentication Protocol according to** [ICAO-9303-2015] **part 11, section 6.1**[103] to prove the identity of the **TOE**[104].

Note

1. SFR FIA_API.1/AA is iterated from PP SFR FIA_API.1/CA ("FIA_API.1").
2. This SFR requires the TOE to implement the Active Authentication Mechanism specified in [ICAO-9303-2015], part 11, section 6.1. The TOE computes a signature over a nonce received from the terminal, sends the signature to the terminal and the terminal verifies the signature.

---

[101] [assignment: authentication mechanism]
[102] [assignment: authorized user or role]
[103] [assignment: authentication mechanism]
[104] [assignment: authorized user or role]

7.6.2.13 FIA_AFL.1/PACE (Authentication failure handling - PACE authentication using non-blocking authorization data)

PACE

Hierarchical to No other components.

Dependencies FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE

FIA_AFL.1.1/PACE The TSF shall detect when **1**[105] unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password.[106]

FIA_AFL.1.2/PACE When the defined number of unsuccessful authentication attempts has been met[107], the TSF shall **delay the next authentication attempt at least 6 seconds.**[108]

Notes

1. With a delay at least 6 seconds a brute force attack lasts in the average more than 30 days even if the password consist only of 6 digits (e.g. the CAN might be so long and consists of digits only).

   The delay applies also when a new session is restarted.

   The MRZ is longer than 6 signs and consists of alpha numerical characters.

7.6.2.14 FIA_AFL.1/RAD (Authentication failure handling – for Signatory PIN)

SSCD

Hierarchical to No other components.

Dependencies FIA_UAU.1 *Timing of authentication*

FIA_AFL.1.1/RAD The TSF shall detect when **an administrator configurable positive integer within 3 up to floor(MINLEN/2) (see note 3. below)**[109] unsuccessful authentication attempts occur related to consecutive failed authentication attempts[110].

FIA_AFL.1.2/RAD When the defined number of unsuccessful authentication attempts has been met[111], the TSF shall block RAD[112] **[REFINEMENT] of the signatory PIN (PIN.QES).**

Notes

1. FIA_AFL.1/RAD amounts to requirement "FIA_AFL.1".
2. The minimal length of the signatory PIN has to be 6.
3. The Administrator configurable positive integer shall not exceed floor(MINLEN/2) where MINLEN denotes the minimal length of the signatory PIN (PIN.QES).
4. With "The TOE stores signatory reference authentication data to authenticate a user as its signatory", see PP [BSI-CC-PP-0059-2009-MA-02], this requirement concerns the PIN of the Signatory (PIN.QES) only.

---

[105] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[106] [assignment: list of authentication events]
[107] [selection: met ,surpassed]
[108] [assignment: list of actions]
[109] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[110] [assignment: list of authentication events]
[111] [selection: met ,surpassed]
[112] [assignment: list of actions]

7.6.2.15 FIA_AFL.1/Suspend_PIN (Authentication failure handling – Suspending PIN)

Hierarchical to No other components.

Dependencies FIA_UAU.1 *Timing of authentication*

FIA_AFL.1.1/Suspend_PIN The TSF shall detect when **2**[113] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts using the PACE password as the shared password for PACE**[114].

FIA_AFL.1.2/Suspend_PIN When the defined number of unsuccessful authentication attempts has been **met**[115], the TSF shall **suspend the reference value of the PACE password according to** [BSI-TR-03110-2-V221].[116]

Note

1. FIA_AFL.1/Suspend_PIN has been adapted from [BSI-CC-PP-0086-2015], *PIN* has been changed to *PACE password*.

7.6.2.16 FIA_AFL.1/Block_PIN (Authentication failure handling – Blocking PIN)

Hierarchical to No other components.

Dependencies FIA_UAU.1 *Timing of authentication*

FIA_AFL.1.1/Block_PIN The TSF shall detect when **1**[117] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts using the suspended**[118] **PACE password as the shared password for PACE**[119].

FIA_AFL.1.2/Block_PIN When the defined number of unsuccessful authentication attempts has been **met**[120], the TSF shall **block the reference value of the PACE password according to** [BSI-TR-03110-2-V221][121].

Note

1. FIA_AFL.1/Block_PIN has been adapted from [BSI-CC-PP-0086-2015], *PIN* has been changed to *PACE password*.

---

[113] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[114] [assignment: list of authentication events]
[115] [selection: met , surpassed]
[116] [assignment: list of actions]
[117] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[118] as required by FIA_AFL.1/Suspend_PIN
[119] [assignment: list of authentication events]
[120] [selection: met , surpassed]
[121] [assignment: list of actions]

7.6.2.17 FIA_AFL.1/AuthAdmin (Authentication failure handling – of administrator for personalization)

Hierarchical to No other components.

Dependencies FIA_UAU.1 *Timing of authentication*

FIA_AFL.1.1/AuthAdmin The TSF shall detect when **5**[122] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts**[123].

FIA_AFL.1.2/AuthAdmin When the defined number of unsuccessful authentication attempts has been **met**[124], the TSF shall **delay the next authentication attempt at least 6 seconds**[125].

Notes

1. FIA_AFL.1/AuthAdmin is added to contents of [BSI-CC-PP-0059-2009-MA-02] (not iterated).
2. This SFR concerns the authentication of the administrator for personalization of the TOE using the Symmetric Authentication Mechanism with Administrator Personalization Key.

7.6.2.18 FIA_API.1 (Authentication proof of identity)

CGA

Hierarchical to No other components.

Dependencies No dependencies.

FIA_API.1.1 The TSF shall provide a **Chip Authentication Protocol Version 1 according to** [BSI-TR-03110-1-V220][126] to prove the identity of the SSCD[127].

Note

1. This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [BSI-TR-03110-1-V220]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [ICAO-9303-2015].

   The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

---

122 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
123 [assignment: list of authentication events]
124 [selection: met , surpassed]
125 [assignment: list of actions]
126 [assignment: authentication mechanism]
127 [assignment: authorized user or role]

7.6.3 Class FDP User Data Protection

The security attributes and related status for the subjects and objects are:

Table 7.6: Subjects and security attributes for access control

Subject or object	Security attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	authorized, not authorized
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value

Note: This ST does not define security attributes for SVD.

7.6.3.1 FDP_ACC.1/TRM (Subset access control)

PACE
EAC

Hierarchical to No other components.

Dependencies FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/TRM The TSF shall enforce the Access Control SFP[128] on terminals gaining access to the User Data and data stored in EF.SOD of the[129] **TOE**[130].

Note

1. The SFR FDP_ACC.1.1/TRM in the current ST covers the definition in PACE PP [BSI-CC-PP-0068-V2-2011-MA-01] and extends it by data stored in EF.SOD of the logical travel document. This extension does not conflict with the strict conformance to PACE PP.
2. This SFR has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01]. The term *travel document* has been changed to *TOE*, because the access control policy also applies eSign applications.

7.6.3.2 FDP_ACF.1/TRM (Security attribute based access control)

PACE
EAC

Hierarchical to No other components.

Dependencies

FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/TRM The TSF shall enforce the Access Control SFP[131] to objects based on the following:

1. Subjects:
   a. Terminal,
   b. BIS-PACE
   c. Extended Inspection System

[128] [assignment: access control SFP]
[129] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[130] REFINEMENT, see note 2 below
[131] [assignment: access control SFP]

2. Objects:
   a. data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical travel document,
   b. data in EF.DG3 of the logical travel document,
   c. data in EF.DG4 of the logical travel document,
   d. all TOE intrinsic secret cryptographic keys stored in the travel document[132]
   e. **data in EF.CardSecurity**[133]
3. Security attributes:
   a. PACE Authentication[134]
   b. **Terminal Authentication Status**[135]
   c. **Terminal Authorization.**[136]

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 BIS-PACE is allowed to read data objects from FDP_ACF.1.1/TRM according to [ICAO-TR-110] after a successful PACE authentication as required by FIA_UAU.1/PACE.[137]

FDP_ACF.1.3/TRM The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.[138]

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

1. Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document.
2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document.
3. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.
4. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM.
5. Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM.
6. Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4.[139]

Notes

[132] e.g. Chip Authentication Version 1 and ephemeral keys

[133] [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]

[134] **REFINEMENT** access control to EF.CardSecurity is added to this SFR

[135] **REFINEMENT** Terminal Authentication v.1, see also Table 7.1 and associated notes

[136] **REFINEMENT** Authorization of the Terminal, , see also Table 7.2 and associated notes

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

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

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

1. The SFR FDP_ACF.1.1/TRM in the current ST covers the definition in PACE PP [BSI-CC-PP-0068-V2-2011-MA-01] and extends it by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in the current ST cover the definition in PACE PP [BSI-CC-PP-0068-V2-2011-MA-01]. The SFR FDP_ACF.1.4/TRM in the current ST covers the definition in PACE PP [BSI-CC-PP-0068-V2-2011-MA-01] and extends it by 3) to 6). These extensions do not conflict with the strict conformance to PACE PP.
2. The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [BSI-TR-03110-1-V220]. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.
3. Please note that the Document Security Object (SO_D) stored in EF.SOD (see [ICAO-9303-2015]) does not belong to the user data, but to the TSF data. The Document Security Object can be read out by Inspection Systems using PACE, see [ICAO-TR-110].
4. FDP_UCT.1/TRM and FDP_UIT.1/TRM require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication Version 1 to the Inspection System. The Password Authenticated Connection Establishment, and the Chip Authentication Protocol v.1 establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).
5. Reading according to FDP_ACF.1.2/TRM includes for a TOE providing Active Authentication the AA public key in EF.DG15.
6. EF.CardSecurity holds the public key needed for authenticating the SSCD during Chip Authentication Protocol Version 1.

7.6.3.3 FDP_RIP.1 (Subset residual information protection)

PACE
SSCD

Hierarchical to No other components.

Dependencies No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from[140] the following objects:

1. Session Keys (immediately after closing related communication session),
2. the ephemeral private key ephem-SK:sub:`PICC-PACE (by having generated a DH shared secret K)`[141]
3. SCD[142]

Notes

1. The SFR FDP_RIP.1.1 just merges the definitions in PP [BSI-CC-PP-0059-2009-MA-02] and [BSI-CC-PP-0068-V2-2011-MA-01] to fulfill both requirements and thereby keeping the strict conformance to the claimed PPs.
2. The TOE shall destroy any session keys in accordance with FCS_CKM.4 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.

[140] [selection: allocation of the resource to, deallocation of the resource from]
[141] [assignment: list of objects]
[142] [assignment: list of objects]

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

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".

7.6.3.4 FDP_UCT.1/TRM (Basic data exchange confidentiality - MRTD)

PACE

Hierarchical to No other components.

Dependencies

[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path] fulfilled by FTP_ITC.1/PACE
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/TRM

FDP_UCT.1.1/TRM The TSF shall enforce the Access Control SFP[143] to be able to transmit and receive[144] user data in a manner protected from unauthorized disclosure.

7.6.3.5 FDP_UIT.1/TRM (Data exchange integrity – Terminal)

PACE

Hierarchical to No other components.

Dependencies

[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

fulfilled by FDP_ACC.1/TRM

FDP_UIT.1.1/TRM The TSF shall enforce the Access Control SFP[145] to be able to transmit and receive[146] user data in a manner protected from modification, deletion, insertion and replay[147] errors.

FDP_UIT.1.2/TRM The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[148] has occurred.

---

143 [assignment: access control SFP(s) and/or information flow control SFP(s)]
144 [selection: transmit, receive]
145 [assignment: access control SFP(s) and/or information flow control SFP(s)]
146 [selection: transmit, receive]
147 [selection: modification, deletion, insertion, replay]
148 [selection: modification, deletion, insertion, replay]

7.6.3.6 FDP_ACC.1/SCD/SVD_Generation (Subset access control)

SSCD

Hierarchical to No other components.

Dependencies FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ SCD/SVD_Generation The TSF shall enforce the SCD/SVD_Generation_SFP[149] on:

1. subjects: S.User,
2. objects: SCD, SVD,
3. operations: generation of SCD/SVD pair.[150]

7.6.3.7 FDP_ACF.1/SCD/SVD_Generation (Security attribute based access control)

SSCD

Hierarchical to No other components.

Dependencies

FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/ SCD/SVD_Generation The TSF shall enforce the SCD/SVD_Generation_SFP[151] to objects based on the following:

the user S.User is associated with the security attribute "SCD/SVD Management".[152]

FDP_ACF.1.2/ SCD/SVD_Generation 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 "authorized" is allowed to generate SCD/SVD pair.[153]

After issuing the TOE S.User is allowed to generate SCD/SVD pair only after successful Chip Authentication Protocol Version 1 following PACE authentication using the PIN.ADMIN as the shared password or after successful EAC with strong certificate following PACE authentication using any PACE password as the shared password.[154]

FDP_ACF.1.3/ SCD/SVD_Generation The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[155]

FDP_ACF.1.4/ SCD/SVD_Generation 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 authorized" is not allowed to generate SCD/SVD pair.[156]

Notes

[149] [assignment: access control SFP]
[150] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[151] [assignment: access control SFP]
[152] [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]
[153] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[154] REFINEMENT
[155] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[156] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

1. The changes represent the need to secure communication between the SSCD Issuing Application and the TOE via trusted channel when generating SCD/SVD pair after issuing the TOE.
2. After the TOE is issued the TOE is in phase OPERATIONAL.

7.6.3.8 FDP_ACC.1/SVD_Transfer (Subset access control)

SSCD

Hierarchical to No other components.

Dependencies FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ SVD_Transfer The TSF shall enforce the SVD_Transfer_SFP[157] on:

1. subjects: S.User,
2. objects: SVD,
3. operations: export.[158]

7.6.3.9 FDP_ACF.1/SVD_Transfer (Subset access control)

SSCD

Hierarchical to No other components.

Dependencies

FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/ SVD_Transfer The TSF shall enforce the SVD_Transfer_SFP[159] to objects based on the following:

1. the S.User is associated with the security attribute Role;
2. the SVD.[160]

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

R.Admin[161] is allowed to export SVD.[162]

After issuing the TOE R.Admin is allowed to export SVD only after successful Chip Authentication Protocol Version 1 following PACE authentication using the PIN.ADMIN as the shared password or after successful EAC with strong certificate following PACE authentication using any PACE password as the shared password.[163]

FDP_ACF.1.3/ SVD_Transfer The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[164].

FDP_ACF.1.4/ SVD_Transfer The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[165].

---

[157] [assignment: access control SFP]
[158] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[159] [assignment: access control SFP]
[160] [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]
[161] [selection: R.Admin, R.Sigy]
[162] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[163] REFINEMENT
[164] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[165] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

Note

1. The changes represent the need to secure communication between the CGA and the TOE via trusted channel when exporting the SVD in Life Cycle Phase "Usage/Operational".

7.6.3.10 FDP_ACC.1/Signature_Creation (Subset access control)

SSCD

Hierarchical to No other components.

Dependencies FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ Signature_Creation The TSF shall enforce the Signature_Creation_SFP[166] on:

1. subjects: S.User,
2. objects: DTBS/R, SCD,
3. operations: signature creation.[167]

7.6.3.11 FDP_ACF.1/Signature_Creation (Security attribute based access control)

SSCD

Hierarchical to No other components.

Dependencies

FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/ Signature_Creation The TSF shall enforce the Signature_Creation_SFP[168] 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"[169]

FDP_ACF.1.2/ Signature_Creation 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".[170]

R.Sigy is only allowed to create electronic signatures for DTBS/R with SCD only after successful PACE authentication using the PIN.CH or CAN as the shared password and successful authentication against RAD.[171]

FDP_ACF.1.3/ Signature_Creation The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.[172]

[166] [assignment: access control SFP]
[167] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[168] [assignment: access control SFP]
[169] [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]
[170] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[171] REFINEMENT
[172] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

FDP_ACF.1.4/ Signature_Creation 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".[173]

Note

1. The changes represent the need to secure communication between the SCA and the TOE via trusted channel for all communication interfaces for when creating electronic signatures for DTBS/R with SCD.

7.6.3.12 FDP_UIT.1/DTBS (Data exchange integrity – DTBS)

SCA

Hierarchical to No other components.

Dependencies

[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1/DTBS The TSF shall enforce the Signature_Creation_SFP[174] to receive[175] user data in a manner protected from modification and insertion[176] errors.

FDP_UIT.1.2/DTBS The TSF shall be able to determine on receipt of user data, whether modification and insertion[177] has occurred.

7.6.3.13 FDP_SDI.2/Persistent (Stored data integrity monitoring and action)

SSCD

Hierarchical to FDP_SDI.1 Stored data integrity monitoring.

Dependencies No dependencies.

FDP_SDI.2.1/Persistent The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[178] on all objects, based on the following attributes: integrity checked stored data[179].

FDP_SDI.2.2/Persistent 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.[180]

---

[173] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[174] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[175] [selection: transmit, receive]
[176] [selection: modification, deletion, insertion, replay]
[177] [selection: modification, deletion, insertion, replay]
[178] [assignment: integrity errors]
[179] [assignment: user data attributes]
[180] [assignment: action to be taken]

7.6.3.14 FDP_SDI.2/DTBS (Stored data integrity monitoring and action)

SSCD

Hierarchical to FDP_SDI.1 Stored data integrity monitoring.

Dependencies No dependencies.

FDP_SDI.2.1/DTBS The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[181] on all objects, based on the following attributes: integrity checked stored DTBS[182].

FDP_SDI.2.2/DTBS 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.[183]

Note

1. 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).

7.6.3.15 FDP_DAU.2/SVD (Data Authentication with Identity of Guarantor)

CGA

Hierarchical to FDP_DAU.1 Basic Data Authentication

Dependencies FIA_UID.1 Timing of identification

FDP_DAU.2.1/SVD The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of SVD[184].

FDP_DAU.2.2/SVD The TSF shall provide CGA with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

Note

1. This SFR only applies for the Life Cycle Phase “Usage/Operational” as the TOE provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.

7.6.4 Class FTP Trusted Path/Channels

7.6.4.1 FTP_ITC.1/PACE (Inter-TSF trusted channel after PACE)

PACE

Hierarchical to No other components.

Dependencies No dependencies.

FTP_ITC.1.1/PACE The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/PACE The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

[181] [assignment: integrity errors]
[182] [assignment: user data attributes]
[183] [assignment: action to be taken]
[184] [assignment: list of objects or information types]

FTP_ITC.1.3/PACE The TSF shall ~~initiate~~ enforce[185] communication via the trusted channel for any data exchange between the TOE and the Terminal.[186]

Notes

1. The trusted IT product is the terminal. In FTP_ITC.1.3/PACE, the word "initiate" is changed to "enforce", as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.
2. The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K.MAC, PACE-K.Enc):

   This secure messaging enforces preventing tracing while Passive Authentication and 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 and FCS_COP.1/PACE_MAC. The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE.
3. Please note that the control on the user data stored in the TOE is addressed by FDP_ ACF.1/TRM
4. If Chip Authentication is successfully performed, secure messaging is immediately started using the derived session keys (CA-K.MAC, CA-K.Enc):

   this secure messaging enforces preventing tracing while the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC.
5. If first PACE session keys are used for establishing the trusted channel and afterward a Chip Authentication is successfully performed, the sessions keys of the CA are used only for the trusted channel (the PACE session keys are not longer used).

7.6.4.2 FTP_ITC.1/SVD (Inter-TSF trusted channel)

CGA

Hierarchical to No other components.

Dependencies No dependencies.

FTP_ITC.1.1/SVD The TSF shall provide a communication channel between itself and another trusted IT product CGA that is logically distinct from other communication channels and provides ensured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SVD The TSF shall permit another trusted IT product[187] to initiate communication via the trusted channel.

FTP_ITC.1.3/SVD The TSF or the CGA shall initiate communication via the trusted channel for

1. data Authentication with Identity of Guarantor according to FIA_API.1 and FDP_DAU.2/SVD,[188]
2. **none**[189].

---

[185] The word "initiate" is changed to "enforce", as the TOE is a passive device that can not initiate the communications.
[186] [assignment: list of functions for which a trusted channel is required]
[187] [selection: the TSF, another trusted IT product]
[188] [assignment: list of functions for which a trusted channel is required]
[189] [assignment: list of other functions for which a trusted channel is required]

Note

1. This SFR only applies for the Life Cycle Phase "Usage/Operational" as the TOE provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase "Usage/Operational".

7.6.4.3 FTP_ITC.1/VAD (Inter-TSF trusted channel – TC Human Interface Device)

SCA

Hierarchical to No other components.

Dependencies No dependencies.

FTP_ITC.1.1/VAD The TSF shall provide a communication channel between itself and another trusted IT product HID that is logically distinct from other communication channels and provides ensured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/VAD The TSF shall permit the remote trusted IT product[190] to initiate communication via the trusted channel.

FTP_ITC.1.3/VAD The TSF or the HID shall initiate communication via the trusted channel for

1. User authentication according to FIA_UAU.1,[191]
2. **none**[192].

Note

1. The PACE protocol used for authentication is a zero-knowledge protocol and thus protects the confidentiality of the VAD implicitly.

7.6.4.4 FTP_ITC.1/DTBS (Inter-TSF trusted channel – Signature creation Application)

SCA

Hierarchical to No other components.

Dependencies No dependencies.

FTP_ITC.1.1/DTBS The TSF shall provide a communication channel between itself and another trusted IT product SCA that is logically distinct from other communication channels and provides ensured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/DTBS The TSF shall permit :ppassigned:` the remote trusted IT product`[193] to initiate communication via the trusted channel.

FTP_ITC.1.3/DTBS The TSF or the SCA shall initiate communication via the trusted channel for

1. signature creation,[194]
2. **none**[195].

[190] [selection: the TSF, another trusted IT product]
[191] [assignment: list of functions for which a trusted channel is required]
[192] [assignment: list of other functions for which a trusted channel is required]
[193] [selection: the TSF, another trusted IT product]
[194] [assignment: list of functions for which a trusted channel is required]
[195] [assignment: list of other functions for which a trusted channel is required]

7.6.5 Class FMT Security Management

Note

1. The SFR FMT_SMR.1/PACE provides basic requirements to the management of the TSF data

7.6.5.1 FMT_SMR.1/PACE (Security roles)

PACE
EAC

Hierarchical to No other components.

Dependencies FIA_UID.1 Timing of identification.

FMT_SMR.1.1/PACE The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Terminal,
4. PACE authenticated BIS-PACE,
5. Country Verifying Certification Authority,
6. Document Verifier,
7. Domestic Extended Inspection System
8. Foreign Extended Inspection System.[196]

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

Notes

1. The SFR FMT_SMR.1.1/PACE in the protection profile [BSI-CC-PP-0056-V2-2012-MA-02] covers the definition in PACE PP [BSI-CC-PP-0068-V2-2011-MA-01] and extends it by 5) to 8). This extension does not conflict with the strict conformance to PACE PP.
2. The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life-cycle phases.

7.6.5.2 FMT_SMR.1 (Security roles)

SSCD

Hierarchical to No other components.

Dependencies FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles R.Admin and R.Sigy[197] **[REFINEMENT] and PACE Terminal**.

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

[196] [assignment: the authorised identified roles]
[197] [assignment: the authorised identified roles]

7.6.5.3 FMT_LIM.1 (Limited capabilities)

PACE
EAC

Hierarchical to No other components.

Dependencies FMT_LIM.2 Limited availability.

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

Deploying Test Features after TOE Delivery does not allow,

1. User Data to be manipulated and disclosed,
2. TSF data to be disclosed or manipulated,
3. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks and[198]
5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.[199]

7.6.5.4 FMT_LIM.2 (Limited availability)

PACE
EAC

Hierarchical to No other components

Dependencies FMT_LIM.1 Limited capabilities.

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

Deploying Test Features after TOE Delivery does not allow:

1. User Data to be 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[200] and
5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.[201]

Notes:

1. The formulation of "Deploying Test Features . . . " in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.
2. Note that the term "software" in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

Note

1. The following SFR are iterations of the component Management of TSF data (FMT_MTD.1).

---

[198] [assignment: the authorised identified roles]
[199] [assignment: Limited capability and availability policy]
[200] [assignment: Limited capability and availability policy]
[201] [assignment: Limited capability and availability policy]

7.6.5.5 FMT_MTD.1/INI_ENA (Management of TSF data - Writing Initialization and Pre-personalization Data)

PACE

Hierarchical to No other components.

Dependencies

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

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to write[202] the Initialization Data and Pre-personalization Data[203] to the Manufacturer[204].

7.6.5.6 FMT_MTD.1/INI_DIS (Management of TSF data - Reading and Using Initialization and Pre-personalization Data)

PACE

Hierarchical to No other components.

Dependencies

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

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to read out[205] the Initialization Data and the Pre-personalization Data[206] to the Personalization Agent[207].

Notes

1. The TOE restricts the ability to write the Initialization Data and the Pre-personalization Data by
   (i) allowing writing these data only once and
   (ii) blocking the role Manufacturer at the end of the manufacturing phase.

   The Manufacturer writes the Initialization Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life cycle phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'OPERATIONAL'. Therefore, read and use access to the Initialization Data and Pre-personalization Data is blocked by the Personalization Agent, before the card is handed out to the travel document holder.
2. With "(i) allowing writing these data only once" the TOE allows to write the Initialization Data and Pre-personalization Data in more than one session but each data only once.

---

[202] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[203] [assignment: list of TSF data]
[204] [assignment: the authorised identified roles]
[205] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[206] [assignment: list of TSF data]
[207] [assignment: the authorised identified roles]

7.6.5.7 FMT_MTD.1/PA (Management of TSF data - Personalization Agent)

PACE

Hierarchical to No other components.

Dependencies

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

FMT_MTD.1.1/PA The TSF shall restrict the ability to write[208] the Document Security Object (SO_D)[209] to the Personalization Agent[210].

Note

1. By writing SO_D into the TOE, the Personalization Agent confirms (on behalf of DS) the correctness and genuineness of all the personalization data related. This consists of user -and TSF- data.

7.6.5.8 FMT_MTD.1/CVCA_INI (Management of TSF data - Initialization of CVCA Certificate and Current Date)

EAC

Hierarchical to No other components.

Dependencies

FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/CVCA_INI The TSF shall restrict the ability to write[211] the

1. initial Country Verifying Certification Authority Public Key: PK.CVCA,
2. initial Country Verifying Certification Authority Certificate: C.CVCA,
3. initial Current Date,
4. **none**[212]

to **Personalization Agent**[213].

Note

1. The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

---

208 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
209 [assignment: list of TSF data]
210 [assignment: the authorised identified roles]
211 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
212 [assignment: list of TSF data]
213 [assignment: the authorized identified roles]

7.6.5.9 FMT_MTD.1/CVCA_UPD (Management of TSF data - Country Verifying Certification Authority)

EAC

Hierarchical to No other components.

Dependencies

FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/CVCA_UPD The TSF shall restrict the ability to update[214] the

1. Country Verifying Certification Authority Public Key: PK.CVCA,
2. Country Verifying Certification Authority Certificate[215]: C.CVCA

to Country Verifying Certification Authority.[216]

Note

1. 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. [BSI-TR-03110-1-V220]). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [BSI-TR-03110-1-V220]).

7.6.5.10 FMT_MTD.1/DATE (Management of TSF data - Current date)

EAC

Hierarchical to No other components.

Dependencies

FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/DATE The TSF shall restrict the ability to modify[217] the Current date[218] to

1. Country Verifying Certification Authority,
2. Document Verifier,
3. Domestic Extended Inspection System.[219]

Note

1. The authorized roles are identified in their certificate (cf. [BSI-TR-03110-1-V220]) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication v.1 (cf. to [BSI-TR-03110-1-V220]).

---

[214] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[215] [assignment: list of TSF data]
[216] [assignment: the authorised identified roles]
[217] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[218] [assignment: list of TSF data]
[219] [assignment: the authorised identified roles]

7.6.5.11 FMT_MTD.1/CA_AA_PK (Management of TSF data - CA and AA Private Key)

EAC

Hierarchical to No other components.

Dependencies

FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/CA_AA_PK The TSF shall restrict the ability to **load**[220] the Chip Authentication Private Key **and Active Authentication Private Key**[221] to **Personalization Agent**[222].

Notes

1. Due to the fact that this SFR is refined with Active Authenticationthe SFR "FMT_MTD.1/CAPK" of [BSI-CC-PP-0056-V2-2012-MA-02] is renamed to "FMT_MTD.1/CA_AA_PK".
2. The verb "load" means here that the Chip Authentication Private Key and the Active Authentication Private Key are generated securely outside the TOE and written into the TOE memory.

7.6.5.12 FMT_MTD.1/CAPK (Management of TSF data - Chip Authentication Private Key)

Hierarchical to No other components.

Dependencies

FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to **load**[223] the Chip Authentication Private Key[224] to **R.Admin**[225] **[REFINEMENT] before issuing the TOE**.

Notes

1. This SFR has been adapted from [BSI-CC-PP-0056-V2-2012-MA-02] .
2. [BSI-CC-PP-0056-V2-2012-MA-02] The verb "load" means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory.
3. The Chip Authentication Private Key mentioned here is used for performing **Chip Authentication Protocol Version 1**.

---

[220] [selection: create, load]
[221] REFINEMENT
[222] [assignment: the authorized identified roles]
[223] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[224] [assignment: list of TSF data]
[225] [assignment: the authorised identified roles]

7.6.5.13 FMT_MTD.1/KEY_READ (Management of TSF data - Key Read)

PACE
EAC

Hierarchical to No other components.

Dependencies

FMT_SMF.1 Specification of management functions **fulfilled by FMT_SMF.1**
FMT_SMR.1 Security roles **fulfilled by FMT_SMR.1**

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to read[226] the

1. PACE passwords,
2. Chip Authentication private key,
3. Personalization Agent Keys[227]
4. **Electronic signature key**
5. **PACE *Chip Authentication Mapping* private key**
6. **Active Authentication Private Key**[228]

to none[229].

Notes

1. The SFR FMT_MTD.1/KEY_READ in the current ST covers the definition in PACE PP [BSI-CC-PP-0068-V2-2011-MA-01] and extends it by additional TSF data. This extension does not conflict with the strict conformance to PACE PP.
2. This SFR makes explicit that the same security function also protects the electronic signature key, the chip authentication mapping key and the active authentication key.

7.6.5.14 FMT_MTD.1/RAD (Management of TSF data)

SSCD

Hierarchical to No other components.

Dependencies

FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/RAD The TSF shall restrict the ability to create[230] the RAD[231] **[REFINEMENT] of the Signatory once** to ~~R.Admin~~[232] **R.Sigy only after successful authentication with the transport PIN (PIN.T).**[233]

Note

1. FMT_MTD.1/RAD captures the requirement "FMT_MTD.1/Admin" but clarifies that by using the transport PIN concept, the creation or the RAD can be bound to the signatory directly instead of using the administrator as an intermediary.

---

226 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
227 [assignment: list of TSF data]
228 [assignment: list of TSF data]
229 [assignment: the authorised identified roles]
230 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
231 [assignment: list of TSF data]
232 [assignment: the authorised identified roles]
233 REFINEMENT of "R.Admin"

7.6.5.15 FMT_MTD.1/Signatory (Management of TSF data)

SSCD

Hierarchical to No other components.

Dependencies

FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Signatory The TSF shall restrict the ability to modify[234] **or unblock**[235] the RAD[236] to R.Sigy[237].

7.6.5.16 FMT_MTD.3 (Secure TSF data)

EAC

Hierarchical to No other components.

Dependencies FMT_MTD.1 Management of TSF data

FMT_MTD.3.1 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.[238]

Refinement: The certificate chain is valid if and only if

1. the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,
2. the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,
3. the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE.

The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.

Note

1. The Terminal Authentication Version 1 is used for Extended Inspection System as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.

---

[234] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[235] [assignment: other operations]
[236] [assignment: list of TSF data]
[237] [assignment: the authorised identified roles]
[238] [assignment: list of TSF data]

7.6.5.17 FMT_SMF.1 (Specification of Management Functions)

PACE
SSCD

Hierarchical to No other components.

Dependencies No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. Initialization,
2. Pre-personalization,
3. Personalization,
4. Configuration
5. creation and modification of RAD;
6. enabling the signature creation function;
7. modification of the security attribute SCD/SVD management, SCD operational;
8. change the default value of the security attribute SCD Identifier;[239]
9. **none.**[240]

Note

1. For "configuration" see chapter *Life Cycle Phases Mapping* section "Phase 3 "Personalization of the travel document" step (v).
2. Items 1. - 4. are defined in the [BSI-CC-PP-0068-V2-2011-MA-01] and items 5. to 8 are defined in [BSI-CC-PP-0059-2009-MA-02].

7.6.5.18 FMT_MOF.1 (Management of security functions behavior)

SSCD

Hierarchical to No other components.

Dependencies

FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to enable[241] the functions signature creation function[242] to R.Sigy[243].

[239] [assignment: list of management functions to be provided by the TSF]
[240] [assignment: list of other security management functions to be provided by the TSF]
[241] [selection: determine the behaviour of, disable, enable, modify the behaviour of]
[242] [assignment: list of functions]
[243] [assignment: the authorised identified roles]

7.6.5.19 FMT_MSA.1/Admin (Management of security attributes)

SSCD

Hierarchical to No other components.

Dependencies

[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/Admin The TSF shall enforce the SCD/SVD_Generation_SFP[244] to restrict the ability to modify[245] **and none**[246] the security attributes SCD/SVD management[247] to R.Admin[248].

7.6.5.20 FMT_MSA.1/Signatory (Management of security attributes)

SSCD

Hierarchical to No other components.

Dependencies

[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/Signatory The TSF shall enforce the Signature_Creation_SFP to restrict the ability to modify the security attributes SCD operational to R.Sigy.

7.6.5.21 FMT_MSA.2 (Secure security attributes)

SSCD

Hierarchical to No other components.

Dependencies

[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for SCD/SVD Management and SCD operational[249].

Security attribute "SCD/SVD Management" can only have the values "authorized" or "not authorized". Both values are secure, depending on the situation.

Security attribute "SCD operational" can only have the values "no" or "yes". Both values are secure, depending on the situation.

The security attribute values are not secure by themselves but in combinations.

The secure values of the combinations are shown in the table *Secure values of the combinations of security attributes*.

[244] [assignment: access control SFP(s), information flow control SFP(s)]
[245] [selection: change_default, query, modify, delete, [assignment: other operations]]
[246] [assignment: other operations]
[247] [assignment: list of security attributes]
[248] [assignment: the authorised identified roles]
[249] [selection: list of security attributes]

Therefore all combinations can be seen as secure.[250]

Table 7.7: Secure values of the combinations of security attributes

SCD/SVD Management	SCD operational	Secure
authorized	yes	YES
authorized	no	YES
not authorized	yes	YES
not authorized	no	YES

7.6.5.22 FMT_MSA.3 (Static attribute initialization)

SSCD

Hierarchical to No other components.

Dependencies

FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the SCD/SVD_Generation_SFP, SVD_Transfer_SFP and Signature_Creation_SFP[251] to provide restrictive[252] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the R.Admin[253] to specify alternative initial values to override the default values when an object or information is created.

7.6.5.23 FMT_MSA.4 (Security attribute value inheritance)

SSCD

Hierarchical to No other components.

Dependencies

[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FMT_MSA.4.1 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.~~[254]

Note

1. Rule 2) is deleted, as the TOE does not support generating an SVD/SCD pair by the signatory alone.

---

250 REFINEMENT
251 [assignment: access control SFP, information flow control SFP]
252 [selection, choose one of: restrictive, permissive, [assignment: other property]]
253 [assignment: the authorised identified roles]
254 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]

7.6.6 Class FAU Security Audit

7.6.6.1 FAU_SAS.1 (Audit storage)

PACE

Hierarchical to No other components.

Dependencies No dependencies.

FAU_SAS.1.1 The TSF shall provide the Manufacturer[255] with the capability to store the Initialization and Pre-Personalization Data[256] in the audit records.

Note

1. The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase 'manufacturing'. The IC manufacturer and the travel document manufacturer in the Manufacturer role write the Initialization and/or Pre-personalization Data as TSF-data into the TOE. The audit records are usually write-only-once data of the travel document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

7.6.7 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMS.1 addresses the inherent leakage.

The SFRs "Limited capabilities (FMT_LIM.1)", "Limited availability (FMT_LIM.2)" together with the SAR "Security architecture description" (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

7.6.7.1 FPT_EMS.1 (TOE Emanation)

PACE
EAC

Hierarchical to No other components.

Dependencies No Dependencies.

FPT_EMS.1.1 The TOE shall not emit

shape and amplitude of signals, time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines during internal operations or data transmissions[257]

in excess of **unintelligible limits**[258] enabling access to

1. Chip Authentication Session Keys
2. PACE session Keys (PACE-K.MAC, PACE-K.Enc),
3. the ephemeral private key ephem-SK.PICC.PACE,
4. **none**[259],
5. Personalization Agent Key(s),
6. Chip Authentication Private Key[260] and

255 [assignment: authorised users]
256 [assignment: list of audit information]
257 [assignment: types of emissions]
258 [assignment: specified limits]
259 [assignment: list of types of TSF data]
260 [assignment: list of types of TSF data]

7. **Active Authentication Private Key** and
8. **PACE *Chip Authentication Mapping* private key**[261].

FPT_EMS.1.2 The TSF shall ensure any users[262] are unable to use the following interface smart card circuit contacts[263] to gain access to

1. Chip Authentication Session Keys
2. PACE Session Keys (PACE-K.MAC, PACE-K.Enc),
3. the ephemeral private key ephem-SK.PICC.PACE,
4. **none**[264],
5. Personalization Agent Key(s) and
6. Chip Authentication Private Key[265] and
7. **Active Authentication Private Key** and
8. **PACE *Chip Authentication Mapping* private key**[266].

Notes

1. This SFR has been adapted from [BSI-CC-PP-0056-V2-2012-MA-02].

   Active Authentication is taken into account in aspect 7, while PACE *Chip Authentication Mapping* has been added as aspect 8.

   These extensions do not conflict with the strict conformance to [BSI-CC-PP-0068-V2-2011-MA-01] and [BSI-CC-PP-0056-V2-2012-MA-02].

2. The TOE preventd 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 or may be originated from internal operation of the TOE or may 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. The travel document's chip can provide a smart card contactless interface and contact-based interface according to ISO/IEC 7816-2 [ISO-IEC-7816-part-2] as well (in case the package only provides a contactless interface the attacker might gain access to the contacts anyway). Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

---

261 [assignment: list of types of user data]
262 [assignment: type of users]
263 [assignment: type of connection]
264 [assignment: list of types of TSF data]
265 [assignment: list of types of TSF data]
266 [assignment: list of types of user data]

7.6.7.2 FPT_EMS.1/SSCD (TOE Emanation of SCD and RAD)

SSCD

Hierarchical to No other components.

Dependencies No dependencies.

FPT_EMS.1.1/SSCD The TOE shall not emit

shape and amplitude of signals, time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines during internal operations or data transmissions[267]

in excess of **unintelligible limits**[268] enabling access to RAD[269] and SCD[270].

FPT_EMS.1.2/SSCD The TSF shall ensure **any users**[271] are unable to use the following interface **smart card circuit contacts**[272] to gain access to RAD[273] and SCD[274].

7.6.7.3 FPT_FLS.1 (Failure with preservation of secure state)

PACE
SSCD

Hierarchical to No other components.

Dependencies No dependencies.

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

1. Exposure to operating conditions causing a TOE malfunction,
2. Failure detected by TSF according to FPT_TST.1,[275]
3. **Failures during cryptographic operations**
4. **Memory failures during TOE execution**
5. **Out of range failures of temperature, clock and voltage sensors**
6. **Failures during random number generation.**[276]

7.6.7.4 FPT_TST.1 (TSF testing)

PACE
SSCD

Hierarchical to No other components.

Dependencies No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests **during initial start-up and at the conditions**

1. **start-up**
2. **Reading Initialization and Pre-personalization Data according to** FMT_MTD.1/INI_DIS
3. **Reading data of LDS groups and EF.SOD**
4. **Reading CA keys (secret key only internally)**

[267] [assignment: types of emissions]
[268] [assignment: specified limits]
[269] [assignment: list of types of TSF data]
[270] [assignment: list of types of user data]
[271] [assignment: type of users]
[272] [assignment: type of connection]
[273] [assignment: list of types of TSF data]
[274] [assignment: list of types of user data]
[275] [assignment: list of types of failures in the TSF]
[276] [assignment: list of other types of failures in the TSF]

5. **Cryptographic key generation according to**

   FCS_CKM.1/DH_PACE_EC **and** FCS_CKM.1/DH_PACE_RSA

   FCS_CKM.1/CA_EC **and** FCS_CKM.1/CA_RSA
6. **Reading certificates internally before Terminal Authentication Protocol v.1 according to** FCS_COP.1/SIG_VER_EC **or** FCS_COP.1/SIG_VER_RSA
7. **Generating random numbers according to** FCS_RNG.1
8. **Generation of the SCD/SVD key pair according to "FCS_CKM.1/EC" or "FCS_CKM.1/RSA"**
9. **Signature-creation according to "FCS_COP.1/EC" or "FCS_COP.1/RSA"**
10. **VAD verification**
11. **RAD modification**[277]

to demonstrate the correct operation of the TSF[278].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of the TSF data[279].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of ~~stored TSF executable code~~ TSF[280].

Note

1. This SFR covers both definitions from [BSI-CC-PP-0059-2009-MA-02] and [BSI-CC-PP-0068-V2-2011-MA-01] which differ only in the selection made in FPT_TST.1.3 by each PP; here the selection of TSF as a whole made by [BSI-CC-PP-0059-2009-MA-02] is the stronger one.

7.6.7.5 FPT_PHP.1 (Passive detection of physical attack)

SSCD

Hierarchical to No other components.

Dependencies No dependencies.

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

[277] [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self test should occur]]
[278] [selection: [assignment: parts of TSF], the TSF]
[279] [selection: [assignment: parts of TSF], TSF data]
[280] [selection: [assignment: parts of TSF], TSF]

7.6.7.6 FPT_PHP.3 Resistance to physical attack

PACE
SSCD

Hierarchical to No other components.

Dependencies No dependencies.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing[281] to the TSF[282] by responding automatically such that the SFRs are always enforced.

Note

1. The TOE implements appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, ‘automatic response’ means here
   (i) assuming that there might be an attack at any time and
   (ii) countermeasures are provided at any time.

7.7 Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the

- Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

- ALC_DVS.2,
- ATE_DPT.2 and
- AVA_VAN.5.

[281] [assignment: physical tampering scenarios]
[282] [assignment: list of TSF devices/elements]

Table 7.8: Security assurance requirements: EAL4 augmented with ALC_DVS.2, ATE-DPT.2 and AVA_VAN.5

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing: security enforcing modules
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Note

1. The TOE shall protect the assets against high attack potential. This includes intermediate storage in the chip as well as secure channel communications established using the Chip Authentication Protocol v.1 (OE.Prot_Logical_Travel_Document). If the TOE is operated in non-certified mode using the BAC-established communication channel, the confidentiality of the standard data shall be protected against attackers with at least Enhanced-Basic attack potential (AVA_VAN.3).

7.8 Security Requirements Rationale

7.8.1 Security Functional Requirements Coverage

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

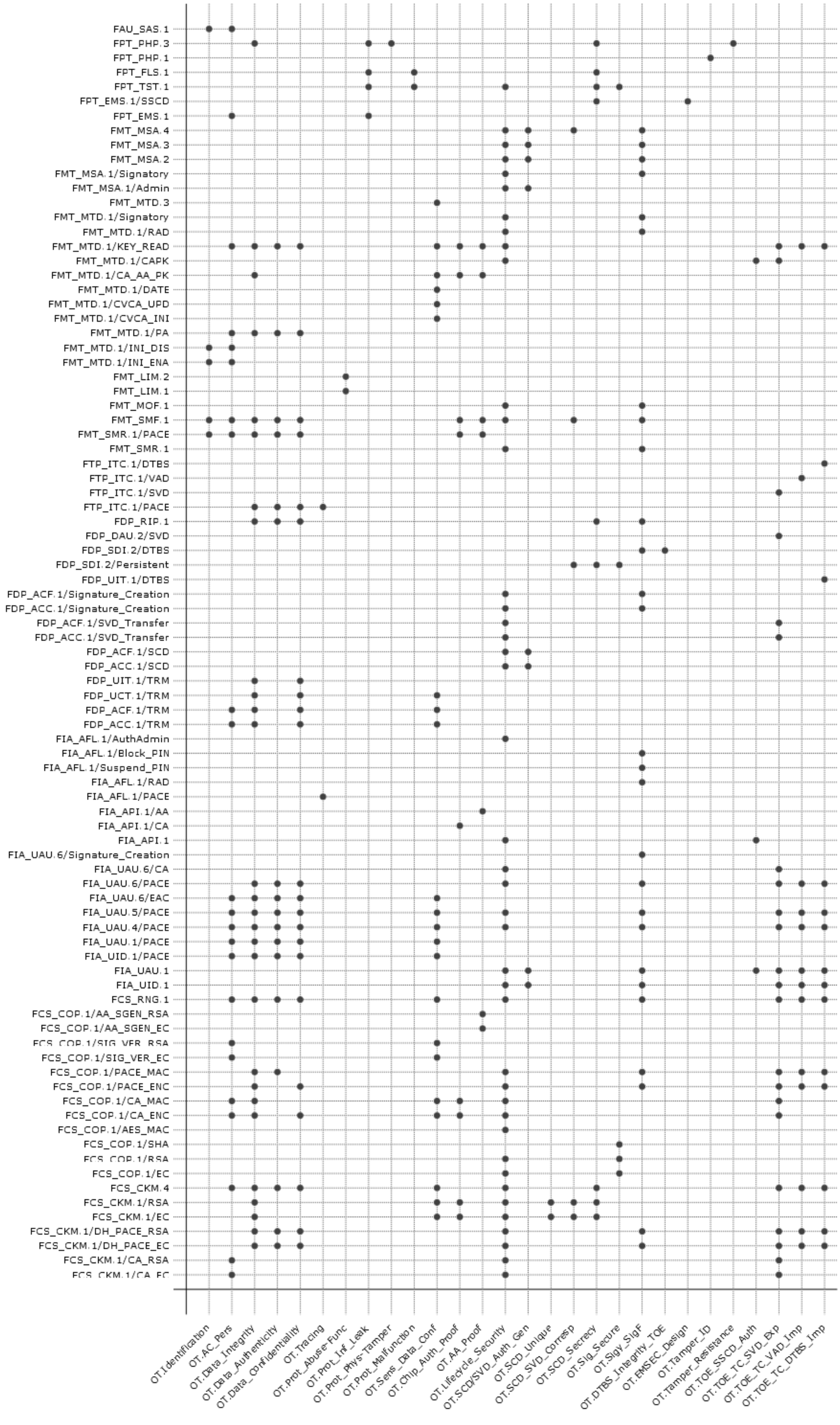

Fig. 7.1: Functional Requirement to TOE security objective mapping

7.8.2 TOE Security Requirements Sufficiency

OT.Identification (Identification of the TOE)

addresses the storage of Initialization and Pre-Personalization Data in its non-volatile memory, whereby they also include the IC Identification Data uniquely identifying the TOE's chip. This will be ensured by TSF according to FAU_SAS.1. The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS requires the Personalization Agent to disable access to Initialization and Pre-personalization Data in the life cycle phase 'operational use'. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

OT.AC_Pers (Access Control for Personalisation of logical MRTD)

addresses the access control of the writing the logical travel document. The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalization Data. The write access to the logical travel document data are defined by the SFR FIA_UID.1/PACE, FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical travel document only once. FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing S.OD and, in generally, personalization data). The SFR FMT_SMR.1/PACE lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The SFRs FMT_MTD.1/KEY_READ and FPT_EMS.1 restrict the access to the Personalization Agent Keys and the Chip Authentication Private Key.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE.

If the Personalization Terminal want to authenticate itself to the TOE by means of the Terminal Authentication Protocol v.1 (after Chip Authentication v.1) with the Personalization Agent Keys the TOE will use TSF according to the FCS_RNG.1 (for the generation of the challenge), FCS_CKM.1/CA_EC **or** FCS_CKM.1/CA_RSA[283] (for the derivation of the new session keys after Chip Authentication v.1), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER_EC **or** FCS_COP.1/SIG_VER_RSA[284] (as part of the Terminal Authentication Protocol v.1) and FIA_UAU.6/EAC (for the re-authentication).

If the Personalization Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the FCS_RNG.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

OT.Data_Integrity (Integrity of Data)

requires the TOE to protect the integrity of the logical travel document stored on the travel document's chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by FPT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1/TRM, FDP_ACF.1/TRM):

Only the Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical travel document (FDP_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical travel document (cf. FDP_ACF.1.4/TRM). FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalization

[283] REFINEMENT FCS_CKM.1/CA_RSA is added to this ST
[284] REFINEMENT FCS_COP.1/SIG_VER_RSA is added to this ST

Agent only and, hence, is to be considered as trustworthy. The Personalization Agent must identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE before accessing these data. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_SMR.1/PACE lists the roles and the SFR ||PP0068 FMT_SMF.1|| lists the TSF management functions.

Unauthorized modifying of the exchanged data is addressed, in the first line, by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. For PACE secured data exchange, a prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE_EC **and** FCS_CKM.1/DH_PACE_RSA[285] and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. The trusted channel is established using PACE, Chip Authentication v.1, and Terminal Authentication v.1. FDP_RIP.1 requires erasing the values of session keys (here: for K.MAC).

The TOE supports the inspection system detect any modification of the transmitted logical travel document data after Chip Authentication v.1. The SFR FIA_UAU.6/EAC and FDP_UIT.1/TRM requires the integrity protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA_EC **or** FCS_CKM.1/CA_RSA[286] (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/CA_AA_PK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterward. The SFR FCS_RNG.1 represents a general support for cryptographic operations needed.

The SFR FCS_RNG.1 **represents a general support for cryptographic operations needed.**[287]

OT.Data_Authenticity (Authenticity of Data)

aims ensuring authenticity of the User- and TSF data (after the PACE Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself.

This objective is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE_EC **and** FCS_CKM.1/DH_PACE_RSA[288] resp. FCS_CKM.1/CA_EC **and** FCS_CKM.1/CA_RSA[289] and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC.

FDP_RIP.1 requires erasing the values of session keys (here: for KMAC).

FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_MTD.1/KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key.

FMT_MTD.1/PA requires that S.OD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalization Agent only and, hence, is to be considered as trustworthy.

The SFR FCS_RNG.1 represents a general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

---

[285] REFINEMENT
[286] REFINEMENT FCS_CKM.1/CA_RSA is added to this ST
[287] REFINEMENT
[288] REFINEMENT
[289] REFINEMENT

OT.Data_Confidentiality (Confidentiality of Data)

aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication resp. Chip Authentication, of these data exchanged.

This objective for the data stored is mainly achieved by (FDP_ACC.1/TRM, FDP_ACF.1/TRM). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used.

This objective for the data exchanged is mainly achieved by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC resp. FCS_COP.1/CA_ENC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE_EC **and** FCS_CKM.1/DH_PACE_RSA[290] resp. FCS_CKM.1/CA_EC **and** FCS_CKM.1/CA_RSA[291] and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for K.enc). The SFR FMT_MTD.1/KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalization Agent only and, hence, is to be considered trustworthy.

The SFR FCS_RNG.1 represents the general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

OT.Sens_Data_Conf (Confidentiality of sensitive biometric reference data)

is enforced by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER_EC **or** FCS_COP.1/SIG_VER_RSA[292].

The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE requires the successful Chip Authentication (CA) v.1 or PACE *Chip Authentication Mapping* before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 the reuse of authentication data is prevented by FIA_UAU.4/PACE. The SFR FIA_UAU.6/EAC and FDP_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_RNG.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA_EC **and** FCS_CKM.1/CA_RSA[293] (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CA_AA_PK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterward.

To allow a verification of the certificate chain as in FMT_MTD.3 the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as of FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.

OT.Chip_Auth_Proof (Proof of the travel document's chip authenticity)

is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1/CA proving the identity of the TOE. The Chip Authentication Protocol v.1 defined by FCS_CKM.1/CA_EC **and** FCS_CKM.1/CA_RSA[294] is performed using a TOE internally stored confidential private key

290 REFINEMENT
291 REFINEMENT
292 REFINEMENT FCS_COP.1/SIG_VER_RSA is added to this ST
293 REFINEMENT
294 REFINEMENT

as required by FMT_MTD.1/CA_AA_PK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol v.1 [BSI-TR-03110-1-V220] requires additional TSF according to FCS_CKM.1/CA_EC **and** FCS_CKM.1/CA_RSA[295] (for the derivation of the session keys), FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging).

The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The SFR FMT_MTD.1/CA_AA_PK **requires that the Chip Authentication Key used for Chip Authentication Protocol v.1 cannot be imported unauthorized.**[296]

OT.AA_Proof (Proof of the travel document's chip authenticity)

is ensured by the Active Authentication Protocol provided by FIA_API.1/AA **proving the identity of the TOE. The Active Authentication Protocol is performed using a TOE internally stored confidential private key as required by** FMT_MTD.1/CA_AA_PK **and** FMT_MTD.1/KEY_READ. **The Active Authentication Protocol** [ICAO-9303-2015] **requires additional TSF according to** FCS_COP.1/AA_SGEN_EC **and** FCS_COP.1/AA_SGEN_RSA **(for the generation ot the digital signatures)**.

The SFRs FMT_SMF.1 **and** FMT_SMR.1/PACE **support the functions and roles related.**

The SFR FMT_MTD.1/CA_AA_PK **requires that the Active Authentication Key used for Active Authentication Protocol cannot be imported unauthorized.**

OT.Prot_Abuse-Func (Protection against Abuse of Functionality)

is ensured by the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other features which may not be used after TOE Delivery.

OT.Prot_Inf_Leak (Protection against Information Leakage)

requires the TOE to protect confidential TSF data stored and/or processed in the travel document's chip against disclosure

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines which is addressed by the SFR FPT_EMS.1,
- by forcing a malfunction of the TOE which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

OT.Tracing (Tracing travel document)

aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ). This objective is achieved as follows:

(i) while establishing PACE communication with CAN or MRZ (non-blocking authorization data) - by FIA_AFL.1/PACE;

(ii) for listening to PACE communication (is of importance for the current ST, since S.OD is card-individual) - FTP_ITC.1/PACE.

[295] REFINEMENT
[296] REFINEMENT

OT.Prot_Phys-Tamper (Protection against Physical Tampering)

is covered by the SFR FPT_PHP.3.

OT.Prot_Malfunction (Protection against Malfunctions)

is covered by

(i) the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and

(ii) the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

OT.Lifecycle_Security (Lifecycle security) is provided by the SFRs

- FCS_CKM.1/EC (for EC SCD/SVD generation),
- FCS_CKM.1/RSA (for RSA SCD/SVD generation),
- FCS_COP.1/EC (for SCD usage using EC),
- FCS_COP.1/RSA (for SCD usage using RSA) and
- FCS_CKM.4 (for SCD destruction)

ensuring cryptographically secure life cycle of the SCD.

The SCD/SVD generation is controlled by TSF according to

- FDP_ACC.1/SCD/SVD_Generation and
- FDP_ACF.1/SCD/SVD_Generation.

The SVD transfer for certificate generation is controlled by TSF according to

- FDP_ACC.1/SVD_Transfer and
- FDP_ACF.1/SVD_Transfer.

The SCD usage is ensured by access control

- FDP_ACC.1/Signature_Creation,
- FDP_ACF.1/Signature_Creation,

which is based on the security attribute secure TSF management according to

- FMT_MOF.1,
- FMT_MSA.1/Admin,
- FMT_MSA.1/Signatory,
- FMT_MSA.2,
- FMT_MSA.3,
- FMT_MSA.4,
- FMT_MTD.1/RAD,
- FMT_MTD.1/Signatory,
- FMT_SMF.1 and
- FMT_SMR.1.

The test functions

- FPT_TST.1

provides failure detection throughout the life cycle.

(Life cycle security) in the Phase “Usage/Preparation” is provided by the SFRs

- FCS_COP.1/AES_MAC,
- FIA_UID.1,
- FIA_UAU.1,
- FIA_AFL.1/AuthAdmin provides protection against brute force attacks against authentication.

(Life cycle security) in the Phase “Usage/Operational” is provided by the SFRs which essentially reflect the fact that the eSign application uses the PACE and Chip Authentication as elementary mechanisms to control the access to the application. The general access control to EF.CardSecurity (references to FDP_ACx.1/TRM) arises from the fact that this EF contains the public key needed to authenticate the SSCD.

- FCS_CKM.1/DH_PACE_EC,
- FCS_CKM.1/DH_PACE_RSA,
- FCS_CKM.1/CA_EC,
- FCS_CKM.1/CA_RSA,
- FCS_CKM.4 (for session key destruction),
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_COP.1/CA_ENC,
- FCS_COP.1/CA_MAC,
- FCS_RNG.1,
- FDP_ACC.1/TRM,
- FDP_ACF.1/TRM,
- FIA_UID.1,
- FIA_UAU.1,
- FIA_UAU.4/PACE,
- FIA_UAU.5/PACE,
- FIA_UAU.6/PACE,
- FIA_UAU.6/CA,
- FIA_API.1,
- FMT_MTD.1/KEY_READ,
- FMT_MTD.1/CAPK.

OT.SCD/SVD_Auth_Gen (Authorised SCD/SVD generation) addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by

- FIA_UID.1 and
- FIA_UAU.1

provide user identification and user authentication prior to enabling access to authorized functions. The SFR

- FDP_ACC.1/SCD/SVD_Generation and
- FDP_ACF.1/SCD/SVD_Generation

provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by

- FMT_MSA.1/Admin,
- FMT_MSA.2 and
- FMT_MSA.3

for static attribute initialization. The SFR

- FMT_MSA.4

defines rules for inheritance of the security attribute "SCD operational" of the SCD.

OT.SCD_Unique (Uniqueness of the signature creation data) implements the requirement of practically unique SCD as laid down in Annex III of the Directive, paragraph 1(a), which is provided by the cryptographic algorithms specified by

- FCS_CKM.1/EC and
- FCS_CKM.1/RSA.

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by

- FCS_CKM.1/EC and
- FCS_CKM.1/RSA

to generate corresponding SVD/SCD pairs. The security functions specified by

- FDP_SDI.2/Persistent

ensure that the keys are not modified, so to retain the correspondence. Moreover, the SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. The management functions identified by

- FMT_SMF.1 and by
- FMT_MSA.4

allow R.Admin to modify the default value of the security attribute SCD Identifier.

OT.SCD_Secrecy (Secrecy of the signature creation data) is provided by the security functions specified by the following SFRs.

- FCS_CKM.1/EC and
- FCS_CKM.1/RSA

ensure the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD.

The security functions specified by

- FDP_RIP.1 and
- FCS_CKM.4

ensure that residual information on SCD is destroyed after the SCD has been used for signature creation and that destruction of SCD leaves no residual information.

The security functions specified by

- FDP_SDI.2/Persistent

ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD.

- FPT_TST.1

tests the working conditions of the TOE and

- FPT_FLS.1

guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA).

- FPT_EMS.1/SSCD and
- FPT_PHP.3

require additional security features of the TOE to ensure the confidentiality of the SCD.

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by

- FCS_COP.1/EC,
- FCS_COP.1/RSA **and**
- FCS_COP.1/SHA

which ensures the cryptographic robustness of the signature algorithms,

- FDP_SDI.2/Persistent

corresponds to the integrity of the SCD implemented by the TOE and

- FPT_TST.1

ensures self-tests ensuring correct signature creation.

FCS_COP.1/SHA is used before FCS_COP.1/EC and FCS_COP.1/RSA if DTBS or an intermediate hash value with the remainder of DTBS (last round hash value) is sent to the TOE for signature creation.

OT.Sigy_SigF (Signature creation function for the legitimate signatory only) is provided by an SFR for identification, authentication and access control.

- FIA_UAU.1 and
- FIA_UID.1

ensure that no signature creation function can be invoked before the signatory is identified and authenticated.

The security functions specified by

- FMT_MTD.1/RAD and
- FMT_MTD.1/Signatory

manage the authentication function.

- FIA_AFL.1/RAD

provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.

- FIA_AFL.1/PACE provides protection against brute force attacks against authentication.
- FIA_AFL.1/Suspend_PIN provides protection against denial-of-service attacks.
- FIA_AFL.1/Block_PIN provides protection against brute force attacks against authentication.

The security functions specified by

- FDP_SDI.2/DTBS

ensures the integrity of stored DTBS and

- FDP_RIP.1

prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process).

The security functions specified by

- FDP_ACC.1/Signature_Creation and
- FDP_ACF.1/Signature_Creation

provide access control based on the security attributes managed according to the SFRs

- FMT_MTD.1/Signatory,
- FMT_MSA.2,
- FMT_MSA.3 and
- FMT_MSA.4.

The SFRs

- FMT_SMF.1 and
- FMT_SMR.1

list these management functions and the roles. These ensure that the signature process is restricted to the signatory.

- FMT_MOF.1

restricts the ability to enable the signature creation function to the signatory.

- FMT_MSA.1/Signatory

restricts the ability to modify the security attributes SCD operational to the signatory.

In the Phase "Usage/Operational" Signature creation function for the legitimate signatory only is additionally provided by the SFRs, which essentially reflects that the PACE protocol is used to protect the signature creation function.

- FCS_CKM.1/DH_PACE_RSA,
- FCS_CKM.1/DH_PACE_EC,
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_RNG.1,
- FDP_UCT.1/TRM,
- FDP_UIT.1/TRM,
- FIA_UID.1,
- FIA_UAU.1,

- FIA_UAU.4/PACE,
- FIA_UAU.5/PACE,
- FIA_UAU.6/PACE and
- FIA_UAU.6/Signature_Creation

OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) ensures that the DTBS/R is not altered by the TOE. The integrity functions specified by

- FDP_SDI.2/DTBS

require that the DTBS/R has not been altered by the TOE.

OT.EMSEC_Design (Provide physical emanations security) covers that no intelligible information is emanated. This is provided by

- FPT_EMS.1/SSCD and
- FPT_EMS.1.

OT.Tamper_ID (Tamper detection) is provided by

- FPT_PHP.1

by the means of passive detection of physical attacks.

OT.Tamper_Resistance (Tamper resistance) is provided by

- FPT_PHP.3

to resist physical attacks.

CGA

OT.TOE_SSCD_Auth (Authentication proof as SSCD) requires the TOE to provide security mechanisms to identify and to authenticate themselves as SSCD[297], which is directly provided by

- FIA_API.1.

The SFR

- FIA_UAU.1

allows (additionally to PP SSCD KG) establishment of the trusted channel before (human) user is authenticated.

Furthermore

- FMT_MTD.1/CAPK

provides the Chip Authentication private key.

CGA

OT.TOE_TC_SVD_Exp (TOE trusted channel for SVD export) requires the TOE to provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA[298], which is directly provided by

[297] This security objective only applies in case a communication channel to the CGA (via trusted channel) in the Life Cycle Phase “Usage/Operational” is needed.
[298] The TOE provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.

- the SVD transfer for certificate generation controlled by TSF according to
  - FDP_ACC.1/SVD_Transfer and
  - FDP_ACF.1/SVD_Transfer.
- The SFR
  - FDP_DAU.2/SVD

  requires the TOE to provide CGA with the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence.
- The SFR
  - FTP_ITC.1/SVD

  requires the TOE to provide a trusted channel to the CGA.

The functionality for integrity and confidentiality is provided by the following SFRs, which reflects that the PACE and CA protocols are used to establish the trusted channel to the CGA.

- FCS_CKM.1/DH_PACE_RSA,
- FCS_CKM.1/DH_PACE_EC,
- FCS_CKM.1/CA_RSA,
- FCS_CKM.1/CA_EC,
- FCS_CKM.4 (for session key destruction),
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_COP.1/CA_ENC,
- FCS_COP.1/CA_MAC,
- FCS_RNG.1,
- FDP_ACC.1/TRM,
- FDP_ACF.1/TRM,
- FDP_UCT.1/TRM,
- FDP_UIT.1/TRM,
- FIA_UID.1,
- FIA_UAU.1,
- FIA_UAU.4/PACE,
- FIA_UAU.5/PACE,
- FIA_UAU.6/PACE,
- FIA_UAU.6/CA,
- FMT_MTD.1/KEY_READ and
- FMT_MTD.1/CAPK.

FDP_RIP.1 requires erasing the values of session keys

SCA

OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import) is provided by

- FTP_ITC.1/VAD

to provide a trusted channel to protect the VAD provided by the HID to the TOE.

The functionality for integrity and confidentiality is provided by the following SFRs which essentially reflects that the PACE protocol is used to protect the VAD

- FCS_CKM.1/DH_PACE_RSA,
- FCS_CKM.1/DH_PACE_EC,
- FCS_CKM.4 (for session key destruction),
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_RNG.1,
- FDP_UCT.1/TRM,
- FDP_UIT.1/TRM,
- FIA_UAU.1,
- FIA_UAU.4/PACE,
- FIA_UAU.5/PACE,
- FIA_UAU.6/PACE and
- FMT_MTD.1/KEY_READ.

FDP_RIP.1 requires erasing the values of session keys

SCA

OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS import) is provided by

- FTP_ITC.1/DTBS

to provide a trusted channel to protect the DTBS provided by the SCA to the TOE and by

- FDP_UIT.1/DTBS

which requires the TSF to verify the integrity of the received DTBS.

The functionality for integrity and confidentiality is provided by the following SFRs which essentially reflects that the DTBS is protected using the PACE protocol.

- FCS_CKM.1/DH_PACE_RSA,
- FCS_CKM.1/DH_PACE_EC,
- FCS_CKM.4 (for session key destruction),
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_RNG.1,
- FDP_UCT.1/TRM,
- FDP_UIT.1/TRM,
- FIA_UID.1,
- FIA_UAU.1,
- FIA_UAU.4/PACE,
- FIA_UAU.5/PACE,
- FIA_UAU.6/PACE and
- FMT_MTD.1/KEY_READ.

FDP_RIP.1 requires erasing the values of session keys

7.9 Satisfaction of Dependencies of Security Requirements

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.

Please note that

- the dependency analysis for SFRs taken over from [BSI-CC-PP-0068-V2-2011-MA-01] has directly been made within the description of each SFR in chapter *Security Functional Requirements for the TOE* and
- these SFRs are not listed in the following table.

Table 7.9 shows the dependencies between the SFR of the TOE.

Table 7.9: Dependencies between the SFR for the TOE

Functional requirements	Dependencies	Satisfied by
FCS_CKM.1/CA_EC	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_CKM.4
FCS_CKM.1/CA_RSA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_CKM.4
FCS_CKM.1/EC	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/EC, FCS_CKM.4
FCS_CKM.1/RSA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/RSA, FCS_CKM.4
FCS_CKM.1/DH_PACE_EC	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_CKM.4
FCS_CKM.1/DH_PACE_RSA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/DH_PACE_EC, FCS_CKM.1/CA_EC, FCS_CKM.1/DH_PACE_RSA, FCS_CKM.1/CA_RSA
FCS_COP.1/CA_ENC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/CA_EC, FCS_CKM.1/CA_RSA, FCS_CKM.4
FCS_COP.1/CA_MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/CA_EC, FCS_CKM.1/CA_RSA, FCS_CKM.4
FCS_COP.1/SIG_VER_EC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	see *Justification* 2 below, FCS_CKM.4
FCS_COP.1/SIG_VER_RSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	see *Justification* 2 below, FCS_CKM.4
FCS_COP.1/AA_SGEN_RSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	see *Justification* 5 below, FCS_CKM.4

continues on next page

Table 7.9 – continued from previous page

Functional requirements	Dependencies	Satisfied by
FCS_COP.1/AA_SGEN_EC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	see *Justification* 5 below, FCS_CKM.4
FCS_COP.1/EC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/EC, FCS_CKM.4
FCS_COP.1/RSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/RSA, FCS_CKM.4
FCS_COP.1/SHA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	see *Justification* 3 below
FCS_COP.1/PACE_ENC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/DH_PACE_EC, FCS_CKM.1/DH_PACE_RSA, FCS_CKM.4
FCS_COP.1/PACE_MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/DH_PACE_EC, FCS_CKM.1/DH_PACE_RSA, FCS_CKM.4
FCS_COP.1/AES_MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	see *Justification* 4 below, FCS_CKM.4
FCS_RNG.1	No dependencies	n.a.
FIA_UID.1[299]	No dependencies	n.a.
FIA_UAU.1[300]	FIA_UID.1	FIA_UID.1
FIA_UAU.6/PACE	No dependencies	n.a.
FIA_UAU.6/CA	No dependencies	n.a.
FIA_AFL.1/RAD	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/PACE	FIA_UAU.1	FIA_UAU.1/PACE
FIA_AFL.1/Suspend_PIN	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/Block_PIN	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/AuthAdmin	FIA_UAU.1	FIA_UAU.1
FIA_API.1	No dependencies	n.a.
FIA_UID.1/PACE	No dependencies	n.a.
FIA_UAU.1/PACE	FIA_UID.1	FIA_UID.1/PACE
FIA_UAU.4/PACE	No dependencies	n.a.
FIA_UAU.5/PACE	No dependencies	n.a.
FIA_UAU.6/EAC	No dependencies	n.a.
FIA_API.1/CA	No dependencies	n.a.
FIA_API.1/AA	No dependencies	n.a.
FDP_ACC.1/TRM	FDP_ACF.1	FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/TRM, see *Justification* 1 below
FDP_ACC.1/SCD/SVD_Generation	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation
FDP_ACF.1/SCD/SVD_Generation	FDP_ACF.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FDP_ACC.1/SVD_Transfer	FDP_ACF.1	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/SVD_Transfer	FDP_ACF.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDP_ACC.1/Signature_Creation	FDP_ACF.1	FDP_ACF.1/Signature_Creation
FDP_ACF.1/Signature_Creation	FDP_ACF.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3

continues on next page

Table 7.9 – continued from previous page

Functional requirements	Dependencies	Satisfied by
FDP_UCT.1/TRM	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1/SVD, FTP_ITC.1/VAD, FTP_ITC.1/DTBS, FDP_ACC.1/TRM
FDP_UIT.1/TRM	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1/SVD, FTP_ITC.1/VAD, FTP_ITC.1/DTBS, FDP_ACC.1/TRM
FDP_UIT.1/DTBS	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1/DTBS, FDP_ACC.1/Signature_Creation
FDP_RIP.1	No dependencies	n.a.
FDP_SDI.2/Persistent	No dependencies	n.a.
FDP_SDI.2/DTBS	No dependencies	n.a.
FDP_DAU.2/SVD	FIA_UID.1	FIA_UID.1
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FMT_SMF.1	No dependencies	n.a.
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_MSA.1	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_SMR.1, FMT_MSA.1	FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation
FMT_MTD.1/RAD	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/Signatory	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/CAPK	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1/PACE
FMT_SMR.1/PACE	FIA_UID.1	FIA_UID.1/PACE
FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
FMT_MTD.1/CVCA_INI	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/CA_AA_PK	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1/PACE

continues on next page

Table 7.9 – continued from previous page

Functional requirements	Dependencies	Satisfied by
FMT_MTD.1/PA	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.3	FMT_MTD.1	FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD
FPT_EMS.1	No dependencies	n.a.
FPT_EMS.1/SSCD	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.
FTP_ITC.1/SVD	No dependencies	n.a.
FTP_ITC.1/VAD	No dependencies	n.a.
FTP_ITC.1/DTBS	No dependencies	n.a.

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

1. The access control TSF according to FDP_ACF.1/TRM uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.
2. (i) **Dependency FCS_CKM.1 is not useful since all keys for Terminal Authentication are generated outside of the TOE, see** *A.Auth_PKI (PKI for Inspection Systems)*.

   (ii) **Dependencies "FDP_ITC.1 Import of user data without security attributes" and "FDP_ITC.2 Import of user data with security attributes" are not necessary because all keys are written using** *FMT_MTD.1/CVCA_INI (Management of TSF data - Initialization of CVCA Certificate and Current Date)* **regardless whether the keys are EC or RSA keys.**[301]
3. Justification of "FCS_COP.1/SHA" can be found in *FCS_COP.1/SHA (Cryptographic operation – Hash calculation)*.
4. Justification of "FCS_COP.1/AES_MAC" can be found in *FCS_COP.1/AES_MAC (Cryptographic operation – MACing with AES)*
5. The Chip Authentication and Active Authentication Keys are permanently stored during personalisation in accordance to FMT_MTD.1/CA_AA_PK. Therefore, no key generation or import policy is needed.

[299] This SFR is amended with an item from [BSI-CC-PP-0068-V2-2011-MA-01].
[300] This SFR is amended with items from PP SSCD KG TCCGA, PP SSCD KG TCSCA and [BSI-CC-PP-0068-V2-2011-MA-01].
[301] REFINEMENT

7.10 Rationale for Chosen Security Assurance Requirements

Table 7.10: Satisfaction of dependencies of security assurance requirements

Assurance requirements	Dependencies	Satisfied by
EAL4 package	(dependencies of EAL4 package are not reproduced here)	By construction, all dependencies are satisfied in a CC EAL package
ALC_DVS.2	No dependencies	
AVA_VAN.5	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1 (all are included in EAL4 package)
ATE_DPT.2	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1	All of these are met or exceeded in the EAL4 assurance package.

The assurance level for PP SSCD KG, PP SSCD KG TCCGA and PP SSCD KG TCSCA is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this ST is just such a product. Augmentation results from the selection of:

- ALC_DVS.2 which provides a higher assurance of the security of the travel document's development and manufacturing especially for the secure handling of the travel document's material.
- ATE_DPT.2 which provides a higher assurance than the pre-defined EAL4 package due to requiring the functional testing of SFR-enforcing modules.
- AVA_VAN.5 which provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential.

The TOE is intended to function as

- an ePassport (with user data stored in an ICAO-compliant ePass application) or
- a SSCD (with user data stored in an eSign application) or
- an eID (with user data stored in an ICAO compliant ePass, an eSign and optionally other eID applications).

Due to the nature of its intended application, i.e. the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

The TOE shall be shown to be highly resistant to penetration attacks.

The requirements of the claimed protection profiles are met or exceeded and the dependencies are fulfilled as shown in Table 7.10.

7.11 Security Requirements - Mutual Support and Internal Consistency

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

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

The dependency analysis in section *Satisfaction of Dependencies of Security Requirements* 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-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in section *Security Functional Requirements for the TOE* are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these 'shared' items.

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

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

8 TOE Summary Specification (ASE_TSS)

8.1 TOE Security Services

8.1.1 User Identification and Authentication (ePass)

This Security Service is responsible for maintaining of the following roles

1. Manufacturer,
2. Personalization Agent,
3. Terminal,
4. PACE authenticated BIS-PACE,
5. Country Verifying Certification Authority,
6. Document Verifier,
7. Domestic Extended Inspection System
8. Foreign Extended Inspection System

according to FMT_SMR.1/PACE.

The TOE allows

- identification of the user according to FIA_UID.1/PACE before the authentication takes place according to FIA_UAU.1/PACE
- the execution of following TSF-mediated actions before the user is identified and associated with one of maintained roles
    1. to establish the communication channel
    2. carrying out the PACE Protocol according to
    3. to read the Initialization Data if it is not disabled by TSF
    4. to carry out the Chip Authentication Protocol v.1
    5. to carry out the Terminal Authentication Protocol v.1
    6. to carry out the Active Authentication Protocol
    7. to run self tests
- the execution of following TSF-mediated actions before the user is authenticated
    1. to establish the communication channel
    2. carrying out the PACE Protocol
    3. to read the Initialization Data if it is not disabled by TSF
    4. to identify themselves by selection of the authentication key
    5. to carry out the Chip Authentication Protocol Version 1
    6. to carry out the Terminal Authentication Protocol Version 1
    7. to carry out the Active Authentication Protocol
    8. to run self tests.

Note

1. If a user acts as (Travel Document) Manufacturer or Personalization Agent, the user acts as Administrator according to [Atos-V60-ADM].

8.1.1.1 Travel document manufacturer Identification and Authentication

After the card leaves the Infineon site the IC Identification Data (a unique IC identifier) written by the IC Manufacturer according to

- FMT_SMF.1 (1)

allows tracing of the travel document.

The travel document manufacturer needs a procedure provided by the developer of the TOE to start his tasks (the card is secured as modeled by FMT_MTD.1/INI_ENA) according to

- FMT_SMF.1 (1) + (2)

which includes import the Initialization Data and Pre-personalization Data in the audit records (FAU_SAS.1) which contains at least the Personalization Agent Key(s) used for the symmetric authentication mechanism (c.f. FCS_COP.1/AES_MAC).

The travel document manufacturer creates also

- file system including MF and ICAO.DF and
- the ePassport application.

Writing the Initialization Data and Pre-personalization Data are managed by FMT_MTD.1/INI_ENA.

With FMT_SMR.1/PACE (1) the TOE maintains the role of the Manufacturer.

Reading of the PACE passwords is not allowed according to FMT_MTD.1/KEY_READ.

8.1.1.2 Personalization Agent Identification and Authentication

With FMT_SMR.1/PACE (2) the TOE maintains the role of the Personalization Agent.

The Personalization Agent is identified and authenticated according to

- FIA_UAU.1/PACE (4)

  and the authentication data is not reused according to

- FIA_UAU.4/PACE (2)

using the Symmetric Authentication Mechanism provided by

- FIA_UAU.5.1/PACE (4)

and the authentication attempt is accepted according to

- FIA_UAU.5.2/PACE rule (2).

The usage of the

- Personalization Agent Key(s)

emit no information about IC power consumption in excess of unintelligible limits and any user is unable to gain access by the card interfaces to this keys according to FPT_EMS.1 (5).

The Personalization Agent performs MRTD Configuration for files (e.g. LDS data groups and EF.SOD) and for objects (e.g. for keys).

The tasks of the Personalization Agent are specified by FMT_SMF.1 (3) + (4).

The Personalization Agent is allowed to read out

- the Initialization Data and the Pre-personalization Data according to FMT_MTD.1/INI_DIS

and he is allowed to read the Initialization Data before he is identificated and authenticated according to

- FIA_UID.1/PACE (3)
- FIA_UAU.1/PACE (3).

Personalization Agent is identified using FIA_UAU.1/PACE (4) by selecting his key.

If the Personalization Agent is identificated and authenticated successfully, he is allowed to perform following tasks:

1. Writing

   (i) initial Country Verifying Certification Authority Public Key: PK.CVCA,

   (ii) initial Country Verifying Certification Authority Certificate: C.CVCA,

   (iii) initial Current Date,

   according to FMT_MTD.1/CVCA_INI

   (iv) the Document Security Object (SO_D)

   according to FMT_MTD.1/PA.

2. Loading

   (v) Chip Authentication Private Key and Active Authentication Private Key

   according to FMT_MTD.1/CA_AA_PK.

   No one is able to read the Chip Authentication Private Key or Active Authentication Private Key after loading it according to FMT_MTD.1/KEY_READ.

3. Loading

   (vi) Chip Authentication Private Key

   according to FMT_MTD.1/CA_AA_PK

   (vii) Active Authentication Private Key

   according to FMT_MTD.1/CA_AA_PK.

   No one is able to read the Chip Authentication Private Key or Active Authentication Private Key after loading it according to FMT_MTD.1/KEY_READ.

   With FPT_TST.1 the TOE checks previously the correct functioning of the cryptographic routines.

Before issuing the TOE to the travel document holder the Personalization Agent

- has to block the read and use access to the Initialization Data.

This is done to prevent misuse, see [BSI-CC-PP-0068-V2-2011-MA-01] application note 49.

Additionally the Personalization Agent shall invalidate his key(s).

8.1.1.3 PACE Terminal Identification and Authentication

With FMT_SMR.1/PACE (3) + (4) the TOE maintains the role of a Terminal and PACE authenticated BIS-PACE.

A user in the role terminal is

- a PACE Terminal after the *PACE or "PACE with CAM" protocol* is successfully performed

using secure messaging in MAC-ENC mode according

- FIA_UAU.5.1/PACE (3).

After the PACE protocol is successfully performed the TOE accepts only commands sent by means of secure messaging according to

- FIA_UAU.5.2/PACE (1).

With FIA_UAU.4/PACE (1) the TOE prevents reuse of authentication data and with FIA_UAU.6/PACE the TOE re-authenticate the PACE Terminal by verifying each commands sent.

A user in the role terminal is allowed to carry out the PACE protocol according to

- FIA_UID.1.1/PACE (2)
- FIA_UAU.1.1/PACE (2)

before the user is identification or authenticated.

After performing PACE protocol the terminal shall perform (depending on it's ability)

- the *Advanced Inspection Procedure with PACE*
- the *Active Authentication Protocol*.

8.1.1.4 Establishing the trusted channel

With FTP_ITC.1/PACE the TOE

- provides a communication channel between itself and another trusted IT product
- permits another trusted IT product to initiate communication via the trusted channel
- enforces communication via the trusted channel for any data exchange between the TOE and the Terminal

which is supported **in case of a PACE protocol** by

- FCS_CKM.1/DH_PACE_EC or FCS_CKM.1/DH_PACE_RSA for PACE session key derivation (with MRZ or CAN as password)

  and

  FIA_UAU.5.1/PACE (3) for secure messaging using

  1. FCS_COP.1/PACE_ENC for confidentiality (by encrypting the data)
  2. FCS_COP.1/PACE_MAC for integrity (by MACing the commands).

or **in case of a Chip Authentication protocol v.1** by

- FCS_CKM.1/CA_EC and FCS_CKM.1/CA_RSA for Chip Authentication session key derivation (using the Chip Authentication Public Key)

  and

  FIA_UAU.5.1/PACE (3) for secure messaging using

  1. FCS_COP.1/CA_ENC for confidentiality (by encrypting the data)
  2. FCS_COP.1/CA_MAC for integrity (by MACing the commands).

and (when transmitting and receiving user data)

- FDP_UCT.1/TRM by protecting from unauthorized disclosure
- FDP_UIT.1/TRM by protecting from modification, deletion, insertion and replay errors and by determining on receipt of user data, whether modification, deletion, insertion and replay has occurred.

After the trusted channel is established the TOE does not execute any command with incorrect message authentication code according to

- FIA_UAU.6/EAC in case of a Chip Authentication protocol v.1
- FIA_UAU.6/PACE in case of a PACE protocol.

The usage of session keys

- {CA-K.MAC, CA-K.Enc} (generated during Chip Authentication)
- {PACE-K.MAC, PACE-K.Enc} (generated during PACE)

and

- ephemeral domain parameters {ephem-SK.PICC.PACE, ephem-PK.PICC.PACE} (used for starting of ECDH for PACE)

emit no information about IC power consumption in excess of unintelligible limits and any user is unable to gain access by the card interfaces to these keys according to FPT_EMS.1 (1) + (2) + (3).

After the trusted channel is terminated the session keys and the ephemeral private key ephem-SK.PICC.PACE are invalidated according to

- FCS_CKM.4
- FDP_RIP.1.

and

- the security attribute PACE Authentication (see FDP_ACF.1.1/TRM) is unset
- the security attribute Terminal Authentication Status is set to “none”.

8.1.2 User Identification and Authentication (eSign)

This security function is responsible for the identification and authentication of the user roles (FMT_SMR.1)

- Administrator
- Signatory
- PACE Terminal

by the methods:

- PACE authentication method[1] according to [BSI-TR-03110-1-V220] and [BSI-TR-03110-2-V221] (FIA_UID.1.1(2), FIA_UAU.1.1(5) and FIA_UAU.5/PACE)
  - It uses
    a. PIN.CH,
    b. optionally PUK.CH,
    c. PIN.T,
    d. PIN.ADMIN or

[1] The PACE authentication method is only applicable in cases where the communication between the TOE and another entity via trusted channel is mandatory.

    e. CAN as passwords.

  - In the first step of the method a random nonce (FCS_RNG.1) encrypted with the password using the cryptographic algorithm AES is transmitted from the TOE to a terminal (FIA_UAU.4/PACE).
  - The method is configured to set the card to a **suspended state** before the password is finally blocked (only PIN.CH, PUK.CH, PIN.T and PIN.ADMIN) (FIA_AFL.1/Suspend_PIN and FIA_AFL.1/Block_PIN) or to **delay the processing** of the authentication command after a failed authentication (CAN) (FIA_AFL.1/PACE).
  - The cryptographic method for confidentiality is AES/CBC (supplied by FCS_COP.1/PACE_ENC).
  - The cryptographic method for authenticity is CMAC (supplied by FCS_COP.1/PACE_MAC).
  - On error (wrong MAC, wrong challenge) the user role is not identified/authenticated.
  - A usage counter of 15-60 prevents the unlimited usage of PUK.CH.
  - On success the session keys are created and stored for Secure Messaging (FCS_CKM.1/DH_PACE).
  - Keys and data in transient memory are overwritten after usage (FCS_CKM.4).

- Secure Messaging (FIA_UAU.1.1(3), FIA_UAU.1.1(4) and FIA_UAU.5/PACE)
  - The cryptographic method for confidentiality is AES/CBC (supplied by FCS_COP.1/PACE_ENC, FCS_COP.1/CA_ENC).
  - The cryptographic method for authenticity is CMAC (supplied by FCS_COP.1/PACE_MAC, FCS_COP.1/CA_MAC).
  - In a Secure Messaging protected command the method for confidentiality and the method for authenticity must be present.
  - A derived session key is used.
  - Any command protected correctly with the session keys is considered to be sent by the successfully authenticated user (FIA_UAU.6/PACE, FIA_UAU.6/CA).
  - On any command that is not protected correctly with the session keys these are overwritten and a new PACE authentication is required.
  - Keys and data in transient memory are overwritten after usage (FCS_CKM.4).
- PIN authentication mechanism using
  - the PIN for qualified signature (PIN.QES) as PIN
    * PIN.QES is a password with a minimum length of 6 digits for authentication data that is blocked after **an administrator configurable positive integer within 3 up to floor(MINLEN/2)** consecutive failed authentication attempts (FIA_AFL.1/RAD)
    * The transmission of the PIN.QES must be protected by Secure Messaging with PACE for all communication interfaces.
- Symmetric Authentication Mechanism (FIA_UID.1.1(3), FIA_UAU.1.1(6), FIA_UAU.4.1/PACE(2), FIA_UAU.5.1/PACE(4) and FIA_UAU.5.2/PACE(2))
  - The cryptographic method for authenticity is CMAC (supplied by FCS_COP.1/AES_MAC).
  - The method is configured to **delay the processing** of the authentication command after consecutive failed authentication attempts (FIA_AFL.1/AuthAdmin).

- Chip Authentication Protocol Version 1[2] according to [BSI-TR-03110-1-V220] (FIA_UAU.5/PACE)
  - The cryptographic method for confidentiality is AES/CBC (supplied by FCS_COP.1/CA_ENC).
  - The cryptographic method for authenticity is CMAC (supplied by FCS_COP.1/CA_MAC).
  - On error the user role is not identified/authenticated.
  - On success the session keys are created and stored for Secure Messaging (FCS_CKM.1/CA).
  - Keys and data in transient memory are overwritten after usage (FCS_CKM.4).
- Passive Authentication[3] for the verification of the authenticity of EF.CardSecurity (FIA_UAU.5/PACE)
  - EF.CardSecurity is signed by the SSCD-provisioning service provider allowing a PACE terminal to verify the authenticity of the TOE.
  - It contains the Chip Authentication Public Key which is used for identifying the SSCD.

The access control methods allow the execution of certain security relevant actions (e.g. self-tests) without successful user identification (FIA_UID.1) and authentication (FIA_UAU.1).

8.1.2.1 Administrator Identification and Authentication

Depending on the life cycle phase the administrator can gain access to the TOE in two different ways:

For the Life Cycle Phase "Personalization":

The administrator is implicitly identified at the beginning of the Phase "Personalization" represented by the TOE life cycle phase MANUFACTURING. Before the administrator is able to start the TOE initialization, the command sequence received by the TOE software developer has to be performed, since the initial StartKey is not known to the administrator. The command sequence changes the secret StartKey (initial StartKey) to a default value ("default" in the sense of "the same value for each SSCD-provisioning service provider") which is known to the administrator. It is mandatory that the administrator change this default value to a value only known to him.

With this administrator-known (but otherwise secret) value for the StartKey, the TOE's life cycle can be switched from the MANUFACTURING to the ADMINISTRATION phase in order to carry out the TOE initialization and TOE personalization which comprises all the tasks performed by an SSCD-provisioning service provider during preparation of the TOE (see section *Life Cycle Phases Mapping* Phase "Personalization").

In order to separate the TOE initialization from the TOE personalization a re-authentication of the administrator is necessary. The TOE is switched from phase ADMINISTRATION to phase OPERATIONAL (permanently) after TOE initialization. The TOE personalization is secured by using the Symmetric Authentication Mechanism with the Administrator Personalization Key which is used to re-authenticate the administrator in order to allow the TOE to be switched back to phase ADMINISTRATION before the personalization tasks can be performed.

[2] The Chip Authentication Protocol Version 1 is only applicable in cases where the communication between the TOE and another entity via trusted channel is mandatory.

[3] Passive Authentication is only applicable in cases where the communication between the TOE and another entity via trusted channel is mandatory.

This TOE behavior is modeled by the SFRs FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS and FMT_MTD.1/PA.

Notes

1. After the TOE has been (permanently) switched to phase OPERATIONAL it is only possible to switch it temporarily to phase ADMINISTRATION. In this sense ADMINISTRATION can be seen rather as a state than as a life cycle phase of the TOE. After a reset the TOE is always in phase OPERATIONAL.
2. The TOE initialization and TOE personalization may only take place in a trusted environment. (A.Env_Admin)

For the Life Cycle Phase "Operational Use":

The administrator is identified and authenticated by using the PACE authentication method **using the PIN.ADMIN as the shared password in the** Phase "Operational Use" **represented by the TOE life cycle phase OPERATIONAL.**

Note

1. By successfully authenticating himself using the PACE authentication method **with PIN.ADMIN as the shared password** the administrator sets the security attribute "SCD/SVD management" to "authorized" (FMT_SMF.1 and FMT_MSA.2).

Before performing any management operations including the generation of the certificate thus including the SVD export from the TOE, the CGA or SSCD Issuing Application establishes the identity of the TOE as SSCD by

- reading and verifying EF.CardSecurity using Passive Authentication (FIA_UAU.5/PACE)
- using the Public Key from EF.CardSecurity together with Chip Authentication Protocol Version 1 to authenticate the SSCD (FIA_API.1).

SCD/SVD generation, SVD export from the TOE in this phase require an interaction with the SSCD-provisioning service provider or certification service provider (CSP) acting as administrator through a trusted channel established by the Chip Authentication Protocol Version 1 (FTP_ITC.1/SVD). (A.Env_Admin and A.CGA).

Additionally management operations, e.g. store certificate info to the SSCD in this phase also require an interaction with the SSCD-provisioning service provider acting as administrator through a trusted channel established by the Chip Authentication Protocol Version 1.

8.1.2.2 Signatory Identification and Authentication

Within the Phase "Operational Use" **represented by the TOE life cycle** phase OPERATIONAL the signatory is identified and authenticated either

- by using the transport PIN (PIN.T) **as the shared password** with the PACE authentication method on first usage upon receiving the TOE from the SSCD-provisioning service provider in order to disable the transport protection and activate (FMT_SMF.1)
    - the PIN for qualified signature (PIN.QES),

- optionally the personal unblocking key (PUK.CH), if present and not already activated.[4]

Notes

1. The transport PIN (PIN.T) cannot be modified and can be used only once.
2. The ability to activate the PIN of the Signatory (PIN.QES) is restricted to the signatory only after disabling the transport protection (FMT_MTD.1/RAD).
3. If the transport PIN is not entered successfully or the transport PIN is blocked, the Signatory cannot be identified or authenticated.
4. If the transport PIN is entered successfully, it is not possible to enter a transport PIN again.
5. If the PIN of the Signatory (PIN.QES) is not set, it is not possible to enter the PIN of the Signatory (PIN.QES) successfully and it is not possible to block the PIN of the Signatory (PIN.QES) with unsuccessful consecutive authentication attempts.

- by using the **optional** personal unblocking key (PUK.CH) **as the shared password** with the PACE authentication method in order to establish a trusted channel between the HID and the TOE for the management environment (FTP_ITC.1/VAD) allowing
  - to unblock the PIN for qualified signature (PIN.QES) while ensuring the confidentiality and integrity of the **VAD** (FMT_MTD.1/Signatory).
  - to unblock the transport PIN (PIN.T[5]) and the card holder PIN (PIN.CH) while ensuring the confidentiality and integrity of the **VAD**.
  - the modification of the personal unblocking key (PUK.CH) and the card holder PIN (PIN.CH) while ensuring the confidentiality and integrity of the **VAD**.

Note

1. PUK.CH must be used as shared password for the PACE authentication method.

- by verifying the PIN for qualified signature (PIN.QES) with the PIN authentication mechanism in order to
  - create qualified electronic signatures,
  - modify the PIN for qualified signature (PIN.QES) itself (FMT_SMF.1 and FMT_MTD.1/Signatory),

---

Note

1. By successfully authenticating himself using PIN verification with the PIN for qualified signature (PIN.QES) the signatory sets the security attribute “SCD operational” to “yes” (FMT_SMF.1 and FMT_MSA.2).

The TOE ensures re-authentication of the signatory for signature creation (FIA_UAU.6/Signature_Creation)

[4] If provision comprises a PUK letter, PUK.CH is already activated.

[5] While PIN.T can only be used successfully once, it is still subject to the PIN suspend and block mechanism. Hence, to avoid denial-of-service attacks on PIN.T, it may be unblocked using PUK.CH.

a) after each signature
   if the personalization allows only a single signature,

b) after card reset or after Application QES was left or before the (N+1)-th signature in a row when limit for consecutive signatures is N
   if the personalization allows a limited number of mass signatures in a row,

c) after card reset or after Application QES was left
   if the personalization allows an unlimited number of mass signatures in a row.

8.1.2.3 PACE Terminal Identification and Authentication

Within the Phase "Operational Use" represented by the TOE life cycle phase OPERATIONAL the PACE Terminal is identified and authenticated by using the PACE authentication method using any of the available shared passwords (PIN.T, PIN.CH, optional PUK.CH, PIN.ADMIN and CAN) in order to establish a trusted channel between the HID and the TOE for both the signing and management environments or between the CGA or an issuer SSCD management application and the TOE for the management environment.

An identified and authenticated PACE Terminal is allowed to access EF.CardSecurity and exchange data with the TOE.

Depending on the shared password used with the PACE authentication method an additional user may be identified and authenticated and additional operations are allowed:

- by using the PACE authentication method **using the** transport PIN (PIN.T) **as the shared password** on first usage upon receiving the TOE from the SSCD-provisioning service provider in order to additionally identify and authenticate the Signatory and establish a trusted channel between the HID and the TOE for disabling the transport protection and activating the RAD (FTP_ITC.1/VAD and FMT_SMF.1).
- by using the PACE authentication method **using the** card holder PIN (PIN.CH) **as the shared password** in order to establish a trusted channel between the HID and the TOE for both the signing and management environments (FTP_ITC.1/VAD and FTP_ITC.1/DTBS) allowing
  - the verification of the PIN for qualified signature (PIN.QES) while ensuring the confidentiality and integrity of the **VAD**,
  - the creation of qualified electronic signatures[6] while ensuring the integrity of the **DTBS** respective **DTBS/R** (A.SCA),
  - the modification of the PIN for qualified signature (PIN.QES)[7] and the card holder PIN (PIN.CH) itself while ensuring the confidentiality and integrity of the **VAD** (FMT_SMF.1).

Notes

1. Using PIN.CH as shared password used with the PACE authentication method only identifies and authenticates the PACE Terminal.
2. For the TOE PIN.CH is only used as shared password for the PACE authentication method.

- by using the PACE authentication method **using the optional** personal unblocking key (PUK.CH) **as the shared password** in order to additionally identify and authenticate the Signatory and establish a trusted channel between the HID and the TOE for the management environment (FTP_ITC.1/VAD) allowing

[6] Additionally requires verification of PIN.QES
[7] Additionally requires verification of PIN.QES

- to unblock the PIN for qualified signature (PIN.QES) while ensuring the confidentiality and integrity of the **VAD** (FMT_MTD.1/Signatory),
- to unblock the transport PIN (PIN.T) and the card holder PIN (PIN.CH) while ensuring the confidentiality and integrity of the **VAD**,
- the modification of the personal unblocking key (PUK.CH) and the card holder PIN (PIN.CH) while ensuring the confidentiality and integrity of the **VAD**.

- by using the PACE authentication method **using the** administrator PIN (PIN.ADMIN) **as the shared password** in order to additionally identify and authenticate the Administrator and establish a trusted channel between the CGA or an issuer SSCD management application and the TOE for management environment (FTP_ITC.1/SVD, FTP_ITC.1/VAD and FTP_ITC.1/DTBS) allowing the execution of Chip Authentication Protocol Version 1.
- by using the PACE authentication method **using** any PACE password **as the shared password** in order to additionally identify and authenticate the Administrator and establish a trusted channel between the CGA or an issuer SSCD management application and the TOE for management environment (FTP_ITC.1/SVD, FTP_ITC.1/VAD and FTP_ITC.1/DTBS) allowing the execution of EAC with strong certificate.
- by using the PACE authentication method **using the** CAN **as the shared password** in order to establish a trusted channel between the HID and the TOE for both the signing and management environments (FTP_ITC.1/VAD and FTP_ITC.1/DTBS) allowing
  - the verification of the PIN for qualified signature (PIN.QES) while ensuring the confidentiality and integrity of the **VAD**,
  - the creation of qualified electronic signatures[8] while ensuring the integrity of the **DTBS** respective **DTBS/R** (A.SCA),
  - the modification of the PIN for qualified signature (PIN.QES)[9] while ensuring the confidentiality and integrity of the **VAD** (FMT_SMF.1),
  - the execution of EAC with strong certificate and the unblocking and modification of the card holder PIN (PIN.CH).
  - to authenticate against PIN.CH, PUK.CH, PIN.T or PIN.ADMIN for the very last retry after setting the relevant password into a suspended state as protection against denial-of-service attacks.

Note

1. The CAN is a non-blocking password with a minimum length of 6 digits that does not effectively represent a secret, but is restricted-revealable.

8.1.2.4 EIS-AIP-PACE Identification and Authentication

An Extended Inspection System (EIS) using successfully the *Advanced Inspection Procedure with PACE* is a EIS-AIP-PACE using a PACE Terminal.

[8] Additionally requires verification of PIN.QES
[9] Additionally requires verification of PIN.QES

8.1.3 Advanced Inspection Procedure with PACE

An Inspection System is an Extended Inspection System after performing the all parts of the Advanced Inspection Procedure (AIP) successfully in this order:

1. The Inspection System uses an identified and authenticated PACE Terminal, see *PACE Terminal Identification and Authentication*,
2. the chip is authenticated successfully to the inspection system, see *Chip Authentication Protocol v.1*
3. the genuineness of the TOE is verified, see *Passive Authentication*
4. the terminal used by inspection system is authenticated successfully to the TOE, see *Terminal Authentication Protocol v.1*

If Advanced Inspection Procedure is performed successfully, the TOE sets the security attributes below (see FDP_ACF.1.1/TRM (3)):

- PACE Authentication
- the security attribute Terminal Authentication Status accordingly to the roles defined in the certificate used for authentication.
- the security attribute Terminal Authorization to the intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.

8.1.4 Protocols

The TOE support the following protocols.

8.1.4.1 PACE or "PACE with CAM" protocol

The TOE accepts authentication using the PACE protocol according to

- FIA_UAU.5.1/PACE (1)

using

- FCS_CKM.1/DH_PACE_EC or FCS_CKM.1/DH_PACE_RSA for PACE session keys

which are also used for establishing the trusted channel, see *Establishing the trusted channel*.

If the terminal uses a wrong password (not derived from MRZ or CAN), the TOE delays the next attempt to establish the PACE protocol at least 5 seconds according to

- FIA_AFL.1/PACE.

This prevents skimming of the passwords because the passwords are non-blocking authorization data.

If the PACE protocol is performed successfully, the TOE sets the security attribute PACE Authentication (FDP_ACF.1.1/TRM (3.a)).

Observe, that the TOE also support the chip-authentication mapping for PACE which combines PACE and the chip authentication protocol into a shorter command exchange between the terminal and the TOE.

8.1.4.2 Chip Authentication Protocol v.1

The terminal proves the identify of the TOE using Chip Authentication Protocol v.1 according to [BSI-TR-03110-1-V220] section "3.4 Chip Authentication Version 1" using

- FIA_API.1/CA and
- FCS_CKM.1/CA_EC and FCS_CKM.1/CA_RSA for Chip Authentication session keys

which are also used for establishing the trusted channel, see *Establishing the trusted channel*.

After the Chip Authentication Protocol v.1 is successfully performed the TOE accepts only commands sent by means of secure messaging according to

- FIA_UAU.5.2/PACE (3).

With FMT_MTD.1/KEY_READ no user is able to read the Chip Authentication Private Key.

After Chip Authentication Protocol v.1 the terminal has to validate the Chip Authentication Public Key by

- performing *Passive Authentication* to verify the genuineness of the TOE.

The usage of the

- Chip Authentication Private Key

emit no information about IC power consumption in excess of unintelligible limits and any user is unable to gain access by the card interfaces to this keys according to FPT_EMS.1 (6).

See *Personalization Agent Identification and Authentication* for the task loading the CA key pair.

8.1.4.3 Active Authentication Protocol

The terminal proves the identify of the TOE using Active Authentication Protocol according to [ICAO-9303-2015] part 11, section 6.1, using

- FIA_API.1/AA

for providing the protocol and

- FCS_COP.1/AA_SGEN_RSA
- FCS_COP.1/AA_SGEN_EC

for signing the terminal's nonce.

With FMT_MTD.1/KEY_READ no user is able to read the Active Authentication Private Key.

The TOE accepts Active Authentication according to

- FIA_UAU.5.1/PACE (6).

After Active Authentication Protocol the terminal has to validate the Active Authentication Public Key by

- performing *Passive Authentication* to verify the genuineness of the TOE.

The usage of the

- Active Authentication Private Key

emit no information about IC power consumption in excess of unintelligible limits and any user is unable to gain access by the card interfaces to this keys according to FPT_EMS.1 (7).

See *Personalization Agent Identification and Authentication* for the task loading the AA key pair.

8.1.4.4 Terminal Authentication Protocol v.1

A terminal authenticates itself to the TOE using the Terminal Authentication Protocol v.1 according to [BSI-TR-03110-1-V220] section "3.5 Terminal Authentication Version 1" using

- FIA_UAU.5.1/PACE (5)

and

- FCS_COP.1/SIG_VER_EC or FCS_COP.1/SIG_VER_RSA

for verifying the certificate chain which is managed by

- FMT_MTD.3 (the certificate chain to the trust anchor must be valid).

With FIA_UAU.5.2/PACE (4) the TOE accepts only authentication attempts using the Chip Authentication Public Key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1, see *Chip Authentication Protocol v.1* and *Establishing the trusted channel*.

With FIA_UAU.4/PACE (3) the TOE prevents reuse of authentication data.

The random nonce is generated using FCS_RNG.1.

With FPT_TST.1 reading of a certificate and the generation of a random nonce is checked previously.

If Terminal Authentication Protocol v.1 is performed successfully, the TOE

1. sets the security attribute Terminal Authentication Status (see FDP_ACF.1.1/TRM) accordingly to the roles defined in the certificate used for authentication. It is possible that the security attribute contains more than one value, e.g. CVCA and IS.
2. sets the security attribute Terminal Authorization to the intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
3. updates the Current Date and trust anchor if necessary, see :*Write access to data of the ePass application at phase Operational Use*

Note

1. Terminal Authentication v.1 can only be performed if Chip Authentication v.1 has been successfully executed.

8.1.4.5 Passive Authentication

The terminal verifies the genuineness of the TOE (MRTD) according to [BSI-TR-03110-1-V220] section "1.1 Passive Authentication" by

- verifying the signature of the SO_D
- reading the hash value of the Chip Authentication public key or the hash value of the Active Authentication public key stored on the chip (LDS data fields)
- comparing the hash values with the hash values computed by the terminal / inspection system over the public keys received from the chip during the respective protocol.

If the hash values are equal and signature is verified, the Passive Authentication is performed successfully.

The TOE accepts Passive Authentication according to

- FIA_UAU.5.1/PACE (2).

For accessing the SO_D and the LDS data fields see *Read access to the data of the ePass application at phase Operational Use*.

Note

1. Performing Passive Authentication by verifying the signature of SO_D and comparing the stored values with hash value computed by the terminal / inspection system cannot be enforced by the TOE.

8.1.5 Access Control (General and ePass)

This security enforces the Access Control SFP on general and ePass application related data.

8.1.5.1 Read access to the data of the ePass application at phase Operational Use

Access to the Logical Travel Document (LTD) and SO_D (EF.SOD) is allowed according to

- FDP_ACC.1/TRM
- FDP_ACF.1/TRM

after *Establishing the trusted channel* according to FDP_ACF.1.4/TRM (2):

1. If security attribute PACE Authentication (FDP_ACF.1.1/TRM (3.a)) is set (i.e. the *PACE or "PACE with CAM" protocol* is performed successfully)

   then

   - the inspection system is allowed to read data objects ((FDP_ACF.1.2/TRM):

   DG1, DG2, DG14, DG15, DG16 and the Security Object SO_D.

2. If security attribute Terminal Authentication Status (FDP_ACF.1.1/TRM (3.b)) has the value "IS" (i.e. the *Advanced Inspection Procedure with PACE* is performed successfully), the inspection system is a Extended Inspection System and allowed to read data objects:

   - DG1, DG2, DG14, DG15, DG16 and the Security Object SO_D
   - DG3 if security attribute Terminal Authorization equals DG3
   - DG4 if security attribute Terminal Authorization equals DG4
   - DG3 and DG4 if security attribute Terminal Authorization equals DG3 / DG4.

Notes

1. If the security attribute Terminal Authorization is set to one of the values "DG3" or "DG4" of "DG3 / DG4" and the terminal is not successfully authenticated as Extended Inspection System, the TOE denies access to data objects 2b) of FDP_ACF.1.1/TRM or data objects 2c) of FDP_ACF.1.1/TRM.
2. If security attribute Terminal Authentication Status is set to one of the values "CVCA" or "DV (domestic)" or "DV (foreign)", the TOE denies any inspection system the access to EF.DG3 or EF.DG4 (FDP_ACF.1.4/TRM (6)).

8.1.5.2 Write access to data of the ePass application at phase Operational Use

With FMT_SMR.1/PACE (5), (6) + (7) the TOE maintains the roles of Country Verifying Certification Authority, Document Verifier and Domestic Extended Inspection System.

The write access to the TOE phase Operational Use depends on role encoded in certificates.

1. A terminal in the role Country Verifying Certification Authority (security attribute terminal authentication status has the value CVCA) is allowed to update (the trust anchor)

- Country Verifying Certification Authority Public Key,
- Country Verifying Certification Authority Certificate

according to FMT_MTD.1/CVCA_UPD if the Country Verifying CA Link-Certificates are valid (FMT_MTD.3) after

- *Terminal Authentication Protocol v.1* is successfully performed.

2. A terminal in the role

- Country Verifying Certification Authority (security attribute terminal authentication status has the value CVCA)

or

- Document Verifier (security attribute terminal authentication status has the value DV (domestic) or DV (foreign))

or

- Domestic Extended Inspection System[10] (security attribute terminal authentication status has the value IS)

is allowed to modify

- the Current Date

according to FMT_MTD.1/DATE if the Country Verifying CA Link-Certificates are valid (FMT_MTD.3) after

- *Terminal Authentication Protocol v.1* is successfully performed

and

- if the Current Date is before the effective date of the respective certificate.

The Current Date is set to the maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates used during performing *Terminal Authentication Protocol v.1*.

If operations (1) and (2) have to be performed both after *Terminal Authentication Protocol v.1*, they are implemented as an atomic operation, see [BSI-TR-03110-3-V221] section "2.5.1 General Procedure".

Please note that a prerequisite for performing successfully TA is a successfully performed *Chip Authentication Protocol v.1*.

[10] From travel document's point of view an Extended Inspection System is a domestic one if the Extended Inspection System is authorized by the issuing State or Organization.

8.1.5.3 General access to data

This aspect of the security function controls

- access to EF.CardSecurity of the TOE and
- data exchange with the TOE.

The TOE allows the access to EF.CardSecurity and data exchange with the TOE if and only if (FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_UCT.1/TRM and FDP_UIT.1/TRM):

1. the access request is sent by an authorized PACE Terminal, see also section *PACE Terminal Identification and Authentication*
2. the access request is sent in a manner protected from unauthorized disclosure, modification, deletion, insertion and replay errors.

8.1.6 AccessControl (eSign)

This security function regulates all access by external entities to operations of the TOE which are only executed after the TSF allowed access. The identification, authentication and association of users to roles is realized by section *User Identification and Authentication (eSign)*.

This security functions also

- restricts the ability to read any keys or passwords (FMT_MTD.1/KEY_READ)
- denies any access not explicitly allowed

8.1.6.1 Access Control provided by the Signature_Creation_SFP

This aspect of the security function is responsible for the realization of the signature creation security function policy (Signature_Creation_SFP) and controls access to the signature creation functionality of the TOE.

The Signature_Creation_SFP is based on the security attribute "SCD operational" which is managed by

- FMT_MSA.1/Signatory
- FMT_MSA.2
- FMT_MSA.3

The TOE allows the creation of electronic signatures for **DTBS/R** with SCD if and only if (FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation, FDP_UIT.1/DTBS, FMT_MOF.1 and FMT_MSA.1/Signatory and FMT_MSA.2):

1. the transport protection is disabled
2. PACE authentication using PIN.CH or CAN as the shared password has been successfully performed
3. the security attribute "SCD/SVD Management" is set to "not authorized" or "authorized"
4. the security attribute "SCD operational" is set to "yes"
5. the signature request is sent by an authorized signatory, see also section *Signatory Identification and Authentication*
6. the signature request is sent in a manner protected from modification and insertion errors

8.1.6.2 Access Control provided by the SCD/SVD_Generation_SFP

This aspect of the security function is responsible for the realization of the SCD/SVD pair generation security function policy (SCD/SVD_Generation_SFP) and controls access to the SCD/SVD pair generation functionality of the TOE.

The SCD/SVD_Generation_SFP is based on the security attribute “SCD/SVD Management” which is managed by

- FMT_MSA.1/Admin
- FMT_MSA.2
- FMT_MSA.3

Depending on the life cycle phase the TOE allows the generation of SCD/SVD pair either by the administrator alone or by the administrator together with the signatory:

For the Life Cycle Phase “Composite Product Integration and Initialization” or “Personalization”:

During the preparation of the TOE (see section *Life Cycle Phases Mapping* Phase “Initialization” and “Personalization”) the TOE allows the (optional) generation of SCD/SVD pair if and only if (FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FMT_MSA.1/Admin, FMT_MSA.2 and FMT_MSA.4):

1. the security attribute “SCD/SVD Management” is set to “authorized”
2. the security attribute “SCD operational” is set to “no”
3. the generation request is sent by an authorized administrator, see also *Administrator Identification and Authentication*

The (re-)generation of the SCD/SVD key pair is also possible in the Phase “Operational use” as detailed in the following section.

For the Life Cycle Phase “Operational use”:

During the operation of the TOE (see section *Life Cycle Phases Mapping* Phase “Operational Use”) the TOE allows the (re-)generation of SCD/SVD pair if and only if (FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FMT_MSA.1/Admin and FMT_MSA.2):

1. PACE authentication using PIN.ADMIN as the shared password has been successfully performed
2. Chip Authentication Protocol Version 1 has been successfully performed
3. the security attribute “SCD/SVD Management” is set to “authorized”
4. the generation request is sent by an authorized administrator, see also section *Administrator Identification and Authentication*

or

1. PACE authentication using any PACE password as the shared password has been successfully performed
2. EAC with strong certificate has been successfully performed
3. the security attribute “SCD/SVD Management” is set to “authorized”
4. the generation request is sent by an authorized administrator, see also section *Administrator Identification and Authentication*

Note

1. Strong Certificate contains Certificate Holder Authorization Template (effective authorization) with right "Install Qualified Certificate" set - see [BSI-TR-03110-4-V221] , chapter 2.2.3.2 Table 4 "Authorization of Authentication Terminals".

8.1.6.3 Access Control provided by the SVD_Transfer_SFP

This aspect of the security function is responsible for the realization of the SVD transfer security function policy (SVD_Transfer_SFP) and controls access to the SVD export functionality of the TOE.

The TOE allows the export of the SVD if and only if (FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer):

1. PACE authentication using PIN.ADMIN as the shared password has been successfully performed
2. Chip Authentication Protocol Version 1 has been successfully performed
3. the export request is sent by an authorized administrator, see also section *Administrator Identification and Authentication*
4. the exported SVD is sent in a manner to provide the CGA with the ability to verify evidence of the validity of the SVD (FDP_DAU.2/SVD).

Note

1. Chip Authentication Protocol Version 1 shall be used in order to provide the CGA with the ability to verify the identity of the SSCD.

or

1. PACE authentication using any PACE password as the shared password has been successfully performed
2. EAC with strong certificate has been successfully performed
3. the export request is sent by an authorized administrator, see also section *Administrator Identification and Authentication*
4. the exported SVD is sent in a manner to provide the CGA with the ability to verify evidence of the validity of the SVD (FDP_DAU.2/SVD).

Note

1. Strong Certificate contains Certificate Holder Authorization Template (effective authorization) with right "Install Qualified Certificate" set - see [BSI-TR-03110-4-V221] , chapter 2.2.3.2 Table 4 "Authorization of Authentication Terminals".

8.1.7 Key management

This security function is responsible for the management of

- the SCD/SVD pair which is used by the signatory to create electronic signatures. This includes the correct generation and the termination of the SCD/SVD pair.
- the Chip Authentication Private Key which is used during Chip Authentication Protocol Version 1 in order to prove the identity of the SSCD.

The TOE supports onboard generation of

a) EC signature key pairs for keys as detailed in *Elliptic curves used* (FCS_CKM.1/EC) and

b) RSA signature key pairs for key as detailed in *RSA key support* (FCS_CKM.1/RSA).

The generation is done with secure values for SCD/SVD parameters so that the key pairs fulfill the corresponding requirements of the standards:

- EC key pairs [ANSI-X9.62], [ISO-IEC-14888-3] and [IEEE-1363] (FCS_CKM.1/EC)
- RSA key pairs [RSA-PKCS1-v2.2] and [IEEE-1363] (FCS_CKM.1/RSA).

The TOE uses the hybrid deterministic random number generator specified by FCS_RNG.1 for the generation of the SCD/SVD pair. The generation is furthermore protected against electromagnetic emanation, power analysis, timing and other side channel attacks, see also section *Protection* below.

In the case that a signature key pair is terminated on request of the signatory, the signature key pair will be deleted by the TOE (FCS_CKM.4).

The SCD is identified by security attribute "SCD identifier". The security attribute "SCD identifier" may have arbitrary values. The Administrator can set/change security attribute "SCD identifier" to a desired value (FMT_SMF.1). The Administrator is thus able to override the default values when an object or information (here: SCD) is created (FMT_MSA.3).

Only during the preparation of the TOE (see section *Life Cycle Phases Mapping* Phase "Personalization") the TOE allows to load the Chip Authentication Private Key if and only if the import request is sent by an authorized administrator, see also section *Administrator Identification and Authentication* (FMT_MTD.1/CAPK).

8.1.8 Signature Creation

This security function is responsible for signature creation using the SCD of the signatory. Before a signature is created by the TOE, the signatory has to be authenticated successfully, see also section *Signatory Identification and Authentication*.

Depending on its configuration the TOE allows to create **single** or **mass** signatures[11].

Note

1. Mass signatures are allowed only in a trusted environment (A.Env_Mass_Signature).

8.1.8.1 Signature Creation with EC

This aspect of the security function creates EC signatures (FCS_COP.1/EC) for hash values using the SCD of the signatory. The signatures created meet the following standards:

- section 7.3 in [ANSI-X9.62],
- section 6.4.3 in [ISO-IEC-14888-3] and
- section 7.2.7 in [IEEE-1363]

  The security function supports EC key lengths of **256, 384, 512, and 521 bits** bits using curves as detailed in section *Elliptic curves used*.

[11] Mass signature generation is used to create either a limited or unlimited number of electronic signatures in a row for an automated process.

8.1.8.2 Signature Creation with RSA

This aspect of the security function creates RSA signatures (FCS_COP.1/RSA) for hash values with PKCS1 or PSS padding using the SCD of the signatory. The signatures created meet the following standards:

- section 5.2.1 RSASP1 in [RSA-PKCS1-v2.2] and
- section 8.2.4 in [IEEE-1363]

The padding is done according to RSASSA-PSS and RSASSA-PKCS1-v1_5.

The security function supports RSA key lengths of the supported key detailed in section *RSA key support* (FCS_COP.1/RSA).

8.1.8.3 TOE IT environment generated hash values

The hash value used for the signature creation is calculated over the DTBS in the TOE IT environment and sent to the TOE under the control of the Signature_Creation_SFP, see section *Access Control provided by the Signature_Creation_SFP*.

8.1.8.4 TOE generated hash values

In case that DTBS instead of a hash value (DTBS/R) is sent to the TOE under the control of the Signature_Creation_SFP, see section *Access Control provided by the Signature_Creation_SFP*, the TOE directly generates a hash value (FCS_COP.1/SHA) over the sent DTBS first which is used afterward for the signature creation.

8.1.8.4.1 Hash last round

In case that the hash value (DTBS/R) is only partly computed in the IT environment an intermediate hash value with the remainder of DTBS is sent to the TOE under the control of the Signature_Creation_SFP, see section *Access Control provided by the Signature_Creation_SFP*. The TOE first computes the 'last round(s)' over the remainder of DTBS and the intermediate hash value (FCS_COP.1/SHA). The final hash value is used afterward for the signature creation.

1. Last round hash values may be used if a signature for large data shall be generated as the IT environment is able to hash much faster than the card.

8.1.9 Test features

According to FMT_LIM.1 and FMT_LIM.2 the TOE is designed in a manner that limits the

- capabilities of TSF
- availability of TSF

to enforce the following policy

> Deploying Test Features after TOE Delivery does not allow,
>
> 1. User Data to be manipulated and disclosed,
> 2. TSF data to be disclosed or manipulated,
> 3. software to be reconstructed,
> 4. substantial information about construction of TSF to be gathered which may enable other attacks and
> 5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.

The Test Features are disabled before the card leaves IC Manufacturer's site.

8.1.10 Protection

This Security Service is responsible for the protection of the TSF, TSF data and user data. The TOE runs a suite of tests to demonstrate the correct operation of the security assumptions provided by the IC platform that underlies the TSF. The following tests are performed during initial start-up (FPT_TST.1):

- The SLC52GDA448* provides a high security initialization software concept. The self test software (STS) is activated by the chip after a cold or warm reset (ISO-reset with I/O=1). It contains diagnostic routines for the chip, see [Infineon-Chip-HW-Ref-16bit-V01], 6.2.4 Power-up and references to *High-security boot-up software (BOS)*.
- After erasure of RAM the state of the User EEPROM is tested and, if not yet initialized, this will be done.
- The User EEPROM heap is checked for consistency. If it is not valid, the TOE will preserve a secure state (life cycle DEATH).
- The backup buffer is checked and its data is restored to User EEPROM, if they were saved because of a command interruption.
- The integrity of stored TSF executable code is verified. If this check fails, the TOE will preserve a secure state (life cycle DEATH).
- The integrity of stored data (objects and files) is verified before their use.
- The hardware sensors, the symmetric coprocessor and the random number generator are tested. If one of the tests fails, the chip platform will perform a security reset.

The TOE will furthermore run tests during

1. start-up
2. Reading Initialization and Pre-personalization Data according to "FMT_MTD.1/INI_DIS"
3. Reading data of LDS groups and EF.SOD
4. Reading CA keys (secret key is used only internally by the TOE)
5. Cryptographic key generation according to "FCS_CKM.1/DH_PACE_EC", "FCS_CKM.1/DH_PACE_RSA", "FCS_CKM.1/CA_EC" and "FCS_CKM.1/CA_RSA"
6. Reading certificates internally before Terminal Authentication Protocol v.1 according to "FCS_COP.1/SIG_VER_EC" or "FCS_COP.1/SIG_VER_RSA"
7. Generating random numbers according to "FCS_RNG.1"
8. the generation of the SCD/SVD pair
9. and during signature creation

according to FPT_TST.1.

The correct operation of generation of the key pairs is demonstrated by performing the following checks:

- Before a random number is used for the generation of a key pair the correct functioning of the random number generator is checked by enforcing all self-test and re-seeding requirements in accordance to *FCS_RNG.1*.

Furthermore the TOE checks

- all command parameters for consistency
- access rights.

If a critical failure occurs during these tests, the TOE will preserve a secure state according to FPT_FLS.1. This comprises the following types of failures:

- Failure of sensors
- Failure of Active Shield
- Failure of cryptographic operation, e.g. during key creation
- Memory failures during TOE execution
- Out of range failures of temperature, clock and voltage sensors
- Failures during random number generation

The TOE is furthermore able to detect physical manipulation and physical probing (FPT_PHP.1 and FPT_PHP.3). This comprises tampering attempts before start-up and during operation. If the underlying IC hardware is attacked by physical or mechanical means, the TOE will respond automatically in form of a continuously generated reset and the TOE functionality will be blocked.

The TOE protects itself against interference and logical tampering by the following measures:

Each application removes its own data from the used memory area at the latest after execution of a command.

- Clearance of sensitive data, as soon as possible (when they are dispensable) according to FCS_CKM.4 and FDP_RIP.1
- No parallel but only serial execution of commands
- Encapsulation of context data (security relevant status variables, etc.)
- Use of the chips MMU (Memory Management Unit)
- Separation of User ROM and Test ROM, where the chip's self test software is located, and to which entries are not possible (apart from cold or warm reset)
- Removal of channel data, when the channel is closed

The TOE protects itself against bypass by not allowing any function in the TSF to proceed if a prior security enforcement function was not executed successfully. The TOE always checks that the appropriate user is successfully authenticated (cf. *User Identification and Authentication (ePass)* and *User Identification and Authentication (eSign)*) for a certain action.

With FPT_EMS.1 and FPT_EMS.1/SSCD the TOE ensures any users are unable to use the following interface smart card circuit contacts to gain access to

- Chip Authentication Session Keys
- PACE Session Keys (PACE-K.MAC, PACE-K.Enc),
- the ephemeral private key ephem-SK.PICC.PACE,
- Personalization Agent Key(s) and
- Chip Authentication Private Key and
- Active Authentication Private Key
- Signature Creation Keys
- the RAD

The TOE provides contact-based and contactless interfaces and is able to connect itself

(i) with terminals which provide a contactless interface

(ii) with terminals which provide a contact-based interface.

In the case that the TOE is connected using it's contactless interface the TOE accepts attempts to establish a connection using it's contact-based interface by

(i) resetting first it's contactless interface

(ii) restarting using it's contact-based interface only.

If the TOE is connected using it's contact-based interface, the TOE does not accept any attempt to establish a connection using it's contactless interface.

The following data persistently stored by TOE has the user data attribute "integrity checked persistent stored data" (FDP_RIP.1):

- SCD
- SVD

Also the DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data" (FDP_RIP.1).

If the integrity of SCD, SVD or DTBS/R is violated, the TOE will prohibit the usage of the altered data and inform the signatory about the integrity error by means of an error code (FDP_SDI.2/Persistent and FDP_SDI.2/DTBS).

8.2 Compatibility between the Composite ST and the Platform-ST

IP_SFR Irrelevant Platform SFR

RP_SFR-SERV Relevant Platform-SFRs being used by the Composite-ST to implement a security service with associated TSFI.

RP_SFR-MECH Relevant Platform SFRs being used by the Composite-ST because of its security properties providing protection against attack to the TOE as a whole

IrOE Objectives for the environment not being relevant for the Composite-ST

CfPOE Objectives for the environment being fulfilled by the Composite-ST automatically, i.e. they can be assigned to TOE security objectives.

SgOE Remaining security objectives for the environment of the Platform-ST not belonging to the group IrOE nor CfPOE and thus need to be addressed in the Composite-ST

The sections

- *Assurance requirements of the composite evaluation*
- *Security objectives for the environment of the platform*
- *Usage of platform TSF by TOE TSF*

show the compatibility of this Composite ST and the Platform-ST as required by [BSI-AIS36-V5].

The Platform-ST is the security target of all controllers SLC52GDA448* used by this TOE as platform.

8.2.1 Assurance requirements of the composite evaluation

The Platform-ST requires

- Common Criteria version v3.1 part 1, part 2 and part 3 and
- EAL6 augmented with the component ALC_FLR.1.

The Composite-ST requires:

- Common Criteria version 3.1, cf. [CC-Part1-V3.1], [CC-Part2-V3.1], and [CC-Part3-V3.1] and
- EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

Therefore the Composite-SAR is a subset of the Platform-SAR.

8.2.2 Security objectives for the environment of the platform

The Platform-ST defined the following objectives for the environment:

- OE.Process-Sec-IC is directly supported by the P.Manufact and the implementing objective OT.Identification which provides means to identify the TOE. Thus, the objective falls in both classes CfPOE and SgOE because it is partially fulfilled by the TOE but also remains partially significant of the composite ST objectives for the environment.
- OE.Lim_Block_Loader, OE.TOE_Auth, and OE.Loader_Usage are not relevant because they are concerned with the authentication of the TOE and the usage of the flash loader in early production phases at the IC manufacturer. Therefore, they are irrelevant objectives fir the environment (IrOE)
- OE.Resp-Appl concerns the treatment of the user data by the Composite-TOE and is enforced intrinsically by the security architecture of the Composite-TOE. Thus, this objective belongs to the automatically fulfilled objectives (CfPOE).

Overall, the objectives for the environment of the platform are fully captured by the Composite-ST.

Thus, the objectives of the Platform-TOE and the Composite-TOE are not contradictory.

8.2.3 Usage of platform TSF by TOE TSF

The relevant SFRs (*RP_SFR-SERV*, *RP_SFR-MECH*) of the platform being used by the Composite ST are listed in the following table.

Table 8.1: Relevant Platform SFRs used as services

RP_SFR-SERV	Meaning	Used by TOE SFR
FRU_FLT.2	Limited Fault Tolerance	FPT_TST.1
FPT_FLS.1	Failure with Preservation of Secure State	FPT_FLS.1
FPT_PHP.3	Resistance to Physical Attack	FPT_PHP.3, FPT_PHP.1
FDP_ITT.1	Basic Internal Transfer Protection	FPT_EMS.1, FPT_EMS.1/SSCD
FDP_IFC.1	Subset Information Flow Control	FPT_EMS.1, FPT_EMS.1/SSCD
FPT_ITT.1	Basic Internal TSF Data Transfer Protection	FPT_EMS.1, FPT_EMS.1/SSCD

continues on next page

Table 8.1 – continued from previous page

RP_SFR-SERV	Meaning	Used by TOE SFR
FCS_RNG.1/TRNG	Quality Metric for Random Numbers	FCS_RNG.1
FPT_TST.2	Subset TOE Security Testing	FPT_TST.1, FPT_PHP.3 (active shield and sensors)
FCS_CKM.1/EC-1	Cryptographic Key Generation (EC)	FCS_CKM.1/EC
FCS_CKM.1/RSA-1	Cryptographic Key Generation (RSA)	FCS_CKM.1/RSA
FCS_COP.1/ECDH-1	Cryptographic Support (ECDH)	FCS_CKM.1/CA_EC, FCS_CKM.1/DH_PACE_EC
FCS_COP.1/ECDSA-1	Cryptographic Support (ECDSA)	FCS_COP.1/SIG_VER_EC, FCS_COP.1/AA_SGEN_EC, FCS_COP.1/EC
FCS_COP.1/RSA-1	Cryptographic Support (RSA)	FCS_COP.1/SIG_VER_RSA, FCS_CKM.1/DH_PACE_RSA, FCS_CKM.1/CA_RSA, FCS_COP.1/AA_SGEN_RSA, FCS_COP.1/RSA
FCS_COP.1/AES-SCL-1 FCS_CKM.4/AES-SCL-1	Cryptographic Support (AES)	FCS_COP.1/CA_ENC (AES), FCS_COP.1/PACE_ENC (AES),
FCS_COP.1/CMAC-SCL-1 FCS_CKM.4/CMAC-SCL-1		FCS_COP.1/CA_MAC (AES), FCS_COP.1/PACE_MAC (AES), FCS_COP.1/AES_MAC
FCS_COP.1/AES		FCS_RNG.1
(FCS_COP.1/HCL)	The SHA implementation is functionally dependent on the underlying crypto library but addressed in the scope of this evaluation as reflected by the addition of FCS_COP.1/SHA in this ST	FCS_CKM.1/CA_EC, FCS_CKM.1/DH_PACE_EC, FCS_CKM.1/DH_PACE_RSA, FCS_CKM.1/CA_RSA
FAU_SAS.1	Audit Storage	FAU_SAS.1
FMT_LIM.1	Limited Capabilities	FMT_LIM.1
FMT_LIM.2	Limited Availability	FMT_LIM.2

Table 8.2: Relevant Platform SFRs used as mechanisms

RP_SFR-MECH	Meaning	Used by TOE SFR
FDP_ACC.1	Subset Access Control	used as supporting mechanism
FDP_ACF.1	Security Attribute Based Access Control	used as supporting mechanism
FDP_SDC.1	Stored date confidentiality	used as supporting mechanism
FDP_SDI.2	Stored data integrity monitoring and action	used as supporting mechanism
FDP_UCT.1	Basic data exchange confidentiality	used as supporting mechanism
FDP_UIT.1	Data exchange integrity	used as supporting mechanism

continues on next page

Table 8.2 – continued from previous page

RP_SFR-MECH	Meaning	Used by TOE SFR
FDP_LIM.1/Loader	Limited Capabilities Loader	used as supporting mechanism
FDP_LIM.2/Loader	Limited Availability Loader	used as supporting mechanism

Any platform SFR neither listed in Table 8.1 nor Table 8.2 is not being used by the Composite ST and thus an irrelevant SFRs (*IP_SFR*).

8.2.4 Conclusion

5890 Overall there is **no conflict** between **security requirements** of this Composite-ST and the Platform-ST.

A Overview of Cryptographic Algorithms

This TOE is a composite product and uses for cryptographic mechanism listed only mechanism provided by the underlying chip SLC52GDA448*. The "Standard of Implementation" is a citation of the ST of the underlying chip SLC52GDA448* only, cf. [Infineon-ST-SLC52-H13].

The following cryptographic algorithms are used by the TOE to enforce its security policy:

Table A.1: Used Algorithms

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments and ST Reference
1	Authenticity	RSA-signature generation (RSA PKCS1_v1_5, RSA PSS), using SHA-256, SHA-384 or SHA-512	[RSA-PKCS1-v2.2], [IEEE-1363]	2048, 3072 and 4096 bits	N/A	Digital signature creation *FCS_COP.1/RSA* (see note 2)
2	Authenticity	ECDSA-signature generation, using SHA-256, SHA-384 or SHA-512 (depending on curve)	[ANSI-X9.62], [ISO-IEC-14888-3], [IEEE-1363], [NIST-FIPS-186-4], [RFC-5639-2010-03]	corresp. to the used elliptic curves: NIST P-256, NIST P-384, NIST P-521, BP P256r1, BP P384r1, BP P512r1	N/A	Digital signature creation *FCS_COP.1/EC* (see note 2)
3	Authenticity, Authentication	Terminal Authentication Version 1, ECDSA-signature verification using SHA-256, SHA-384 or SHA-512	[ANSI-X9.62] section 7.4.1, [ISO-IEC-14888-3] section 6.4.4, and [IEEE-1363] section 7.2.8 (Refer to Cryptographic Primitives for the definition of the hash-functions)	corresp. to the used elliptic curves: NIST P-256, NIST P-384, NIST P-521, BP P256r1, BP P384r1, BP P512r1	[ICAO-9303-2015], [BSI-TR-03110-3-V221]	*FCS_COP.1/SIG_VER_EC* (see notes 1 and 9)

continues on next page

Table A.1 – continued from previous page

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments and ST Reference
4	Authenticity, Authentication	Terminal Authentication Version 1, RSA-signature verification using SHA-256, SHA-384 or SHA-512	[RSA-PKCS1-v2.2], section 5.2.2 RSAVP1, padding according to RSASSA-PSS or RSASSA-PKCS1-v1_5 (Refer to Cryptographic Primitives for the definition of the hash-functions)	2048 and 3072 bits	[ICAO-9303-2015], [BSI-TR-03110-3-V221]	*FCS_COP.1/SIG_VER_RSA* (see notes 1 and 10)
5	Authentication	PACEv2 (Generic Mapping, Integrated Mapping[1], Chip Authentication Mapping), *PACE*	[BSI-TR-03110-1-V220] (PACE v2)	128 (nonce), 160 (*MRZ*), PINs: 48..128 (PIN.CH, *CAN*), 64..128 (PUK.CH), 40 (PIN.T), 192..256 (PIN.ADMIN)	[ICAO-TR-110], [BSI-TR-03110-1-V220]	*FCS_CKM.1/DH_PACE_RSA*, *FCS_CKM.1/DH_PACE_EC* (see notes 3 and 11)
6	Authentication	Symmetric Authentication, AES in CMAC mode	[NIST-FIPS-197] (AES), [ISO-IEC-9797-1-2011] algorithm 5 and padding method 2 (CMAC)	192	[ICAO-TR-110], [BSI-TR-03110-1-V220]	*FCS_COP.1/AES_MAC* (see note 4)

continues on next page

Table A.1 – continued from previous page

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments and ST Reference
7	Authentication	Active Authentication, ECDSA signature generation using SHA-256, SHA-384 or SHA-512	According to [ANSI-X9.62] section 7.3 and according to [ISO-IEC-14888-3], section 6.4.3, and [IEEE-1363], section 7.2.7. (Refer to Cryptographic Primitives for the definition of the hash-functions)	corresp. to the used elliptic curves: NIST P-256, NIST P-384, NIST P-521, BP P256r1, BP P384r1, BP P512r1	[ICAO-9303-2015]	*FCS_COP.1/AA_SGEN_EC* (see notes 2 and 9)
8	Authentication	Active Authentication, RSA signature generation using SHA-256	According to section 5.2.1 RSASP1 in [RSA-PKCS1-v2.2] for u = 2; padding according to ISO/IEC 9796-2 (Refer to Cryptographic Primitives for the definition of the hash-functions)	2048, 3072 and 4096 bits	[ICAO-9303-2015]	*FCS_COP.1/AA_SGEN_RSA* (see note 2 and 10)

continues on next page

PUBLIC

Table A.1 – continued from previous page

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments and ST Reference
9	Key Generation	EC signature key pair generation	ECDSA Key Generation [ANSI-X9.62], appendix A4.3, [ISO-IEC-14888-3], section 6.4.2 and [IEEE-1363], appendix A.16.9	corresp. to the used elliptic curves: NIST P-256, NIST P-384, NIST P-521, BP P256r1, BP P384r1, BP P512r1	N/A	*FCS_CKM.1/EC* (see note 3)
10	Key Generation	RSA signature key pair generation	Proprietary. Generated keys meet [RSA-PKCS1-v2.2], sections 3.1 and 3.2 and [IEEE-1363], section 8.1.3.1	2048, 3072 and 4096 bits	N/A	*FCS_CKM.1/RSA* (see note 3)
11	Key Agreement	PACE Key derivation ECDH using SHA-1 and SHA-256	[ICAO-TR-110], [BSI-TR-03111-V210-ECC]	128 (AES), 192 (AES), 256 (AES)	[ICAO-TR-110], [BSI-TR-03110-1-V220]	*FCS_CKM.1/DH_PACE_EC*
12	Key Agreement	PACE Key derivation DH using SHA-1 and SHA-256	[RSA-PKCS-3-V1.4] (Refer to Cryptographic Primitives for the definition of the hash-functions)	128 (AES), 192 (AES), 256 (AES)	[ICAO-TR-110], [BSI-TR-03110-1-V220]	*FCS_CKM.1/DH_PACE_RSA*

continues on next page

Table A.1 – continued from previous page

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments and ST Reference
13	Key Agreement, Authentication	Chip Authentication Version 1, ECDH Key agreement and key derivation using SHA-1 and SHA-256	[ICAO-TR-110] [BSI-TR-03111-V210-ECC] (Refer to Cryptographic Primitives for the definition of the hash-functions)	128 (AES), 192 (AES), 256 (AES), 256 (EC), 384 (EC), 512 (EC), 521 (EC)	[ICAO-TR-110], [BSI-TR-03110-1-V220]	*FCS_CKM.1/CA_EC*
14	Key Agreement, Authentication	Chip Authentication Version 1, DH Key agreement and key derivation using SHA-1 and SHA-256	[RSA-PKCS-3-V1.4] (Refer to Cryptographic Primitives for the definition of the hash-functions)	128 (AES), 192 (AES), 256 (AES), 2048 (RSA)	[BSI-TR-03110-1-V220]	*FCS_CKM.1/CA_RSA* (see note 8)
15	Confidentiality	Secure Messaging, AES in CBC mode	[NIST-FIPS-197] (AES), [NIST-800-38A-2001], section 6.2 (CBC)	128, 192, 256	[ICAO-TR-110], [BSI-TR-03110-1-V220]	*FCS_COP.1/PACE_ENC*, *FCS_COP.1/CA_ENC* (see note 4)
16	Integrity	Secure Messaging, AES in CMAC mode	[NIST-FIPS-197] (AES), [ISO-IEC-9797-1-2011] algorithm 5 and padding method 2 (CMAC)	128, 192, 256	[ICAO-TR-110], [BSI-TR-03110-1-V220]	*FCS_COP.1/PACE_MAC*, *FCS_COP.1/CA_MAC* (see note 4)
17	Trusted Channel	Secure Messaging in ENC MAC mode established during PACE	[BSI-TR-03110-1-V220]	see lines “PACE Key Derivation DH” and “PACE Key Derivation ECDH” of this table	[ICAO-TR-110], [BSI-TR-03110-1-V220]	*FTP_ITC.1/SVD*, *FTP_ITC.1/VAD*, *FTP_ITC.1/DTBS*, *FTP_ITC.1/PACE*

continues on next page

PUBLIC

Table A.1 – continued from previous page

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key size in bits	Standard of Application	Comments and ST Reference
18	Trusted Channel	Secure Messaging in ENC MAC mode established during CA after PACE	[BSI-TR-03110-1-V220]	see lines "CA DH Key agreement and key derivation" and "CA ECDH Key agreement and key derivation" of this table	[ICAO-TR-110], [ICAO-9303-2015], [BSI-TR-03110-1-V220]	*FTP_ITC.1/SVD*, *FTP_ITC.1/PACE*
19	Cryptographic Primitive	DRG.4 random number generator	[NIST-SP800-90A] CTR_DRBG, using AES as block cipher, random source of class PTG.2 according to [BSI-AIS31-V3]	./.	N/A	*FCS_RNG.1* (see note 5)
20	Cryptographic Primitive	SHA-1, SHA-256, SHA-384, SHA-512	[NIST-FIPS-180-4]	./.	[BSI-TR-03110-1-V220]	Signature verification, signature generation, key derivation (see notes 6 and 7)

Notes

1. This TOE uses the Infineon libraries RSA, ECC and Toolbox (ACL52 v2.08.007), SHA (HCL52 v1.12.001) and Symmetric Crypto Library (SCL52 v2.04.002) of the underlying chip SLC52GDA448*. For the standard of implementation of "digital signature verification" using RSA or EC see [Infineon-ST-SLC52-H13].
2. This TOE uses the Infineon libraries RSA, ECC and Toolbox (ACL52 v2.08.007), SHA (HCL52 v1.12.001) and Symmetric Crypto Library (SCL52 v2.04.002) of the underlying chip SLC52GDA448*. For the standard of implementation of "digital signature generation" using RSA or EC see [Infineon-ST-SLC52-H13].
3. This TOE uses the Infineon libraries RSA, ECC and Toolbox (ACL52 v2.08.007), SHA (HCL52 v1.12.001) and Symmetric Crypto Library (SCL52 v2.04.002) of the underlying chip SLC52GDA448*. For the "cryptographic key generation algorithm" for RSA, EC and ECDH see [Infineon-ST-SLC52-H13].

[1] Integrated Mapping is a licensed technology protected by IDEMIA under the patents FR2946818 and FR2946819 and their foreign extensions.

4. This TOE uses the Infineon libraries RSA, ECC and Toolbox (ACL52 v2.08.007), SHA (HCL52 v1.12.001) and Symmetric Crypto Library (SCL52 v2.04.002) of the underlying chip SLC52GDA448*. For the standard of implementation of "Advanced Encryption Standard (AES)" see [Infineon-ST-SLC52-H13].
5. This TOE uses the random numbers generation provided by the underlying chip SLC52GDA448* as random source for the hybrid deterministic random number generator. For the standard of implementation of "random numbers generation Class DRG.4 according to [BSI-AIS2031-RNG-CLASSES-V2]" see [Infineon-ST-SLC52-H13].
6. This TOE uses the Infineon libraries RSA, ECC and Toolbox (ACL52 v2.08.007), SHA (HCL52 v1.12.001) and Symmetric Crypto Library (SCL52 v2.04.002) of the underlying chip SLC52GDA448*. For the standard of implementation of hash algorithms SHA-{256, 384, 512} see [Infineon-Chip-HCL52].
7. This TOE uses the Infineon libraries RSA, ECC and Toolbox (ACL52 v2.08.007), SHA (HCL52 v1.12.001) and Symmetric Crypto Library (SCL52 v2.04.002) of the underlying chip SLC52GDA448*. For the standard of implementation of hash algorithms SHA-1 see [Infineon-Chip-HCL52].
8. This TOE uses the Infineon libraries RSA, ECC and Toolbox (ACL52 v2.08.007), SHA (HCL52 v1.12.001) and Symmetric Crypto Library (SCL52 v2.04.002) of the underlying chip SLC52GDA448*. For computing the shared secret via the modular exponentiation function (`CryptoRsaSignExpMask()`) of the RSA crypto library is used. Function `CryptoRsaSignExpMask()` of RSA crypto library is used also for signing.
9. EC curves for TA and AA are taken from [BSI-TR-03110-3-V221] Table 4: Standardized Domain Parameters.
10. The RSA bit lengths for TA and AA are taken over from [BSI-TR-03110-3-V221] section A.7.3.2. Public Key Format.
11. Regarding the supported lengths for PIN.CH (6..16 Byte), PUK.CH (8..16 Byte), PIN.T (5 Byte), *CAN* (6..16 Byte) and PIN_ADMIN (24..32 Byte) refer to the guidance documentation.

Bibliography

[CC-Part1-V3.1] CCMB-2017-04-001, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Common Criteria Maintenance Board, Version 3.1, Revision 5, 2017-04.

[CC-Part2-V3.1] CCMB-2017-04-002, Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Common Criteria Maintenance Board, Version 3.1, Revision 5, 2017-04.

[CC-Part3-V3.1] CCMB-2017-04-003, Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Common Criteria Maintenance Board, Version 3.1, Revision 5, 2017-04.

[CEM-V3.1] CCMB-2017-04-004, Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, 2017-04.

[CC-CompositeEval-Smart-Cards] Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0 Revision 1, CCDB-2007-09-001.

[BSI-AIS2031-RNG-CLASSES-V2] AIS 20 / AIS 31, A proposal for: Functionality classes for random number generators, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.0, 2011-09-18.

[BSI-AIS36-V5] AIS 36, Anwendungshinweise und Interpretationen zum Schema, AIS36: Kompositionsevaluierung, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 5, 2017-03-15.

[BSI-AIS31-V3] AIS 31, Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 3, 2013-05-15.

[BSI-CC-PP-0055-110] Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application" Basic Access Control, BSI-CC-PP-0055 Version 1.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-03-25.

[BSI-CC-PP-0059-2009-MA-02] Protection profiles for Secure signature creation device - Part 2: Device with key generation, Information Society Standardization System CEN/ISSS, EN 419211-2:2013, 2013-07-17.

[BSI-CC-PP-0071-2012-MA-01] Protection profiles for Secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application, Information Society Standardization System CEN/ISSS, EN 419211-4:2013, 2013-11-27

[BSI-CC-PP-0072-2012-MA-01] Protection profiles for Secure signature creation device - Part 5: Extension for device with key generation and trusted communication with signature creation application, Information Society Standardization System CEN/ISSS, EN 419211-5:2013, 2013-12-04.

[BSI-CC-PP-0056-V2-2012-MA-02] Assurance Continuity Maintenance Report BSI-CC-PP-0056-V2-2012-MA-02 for Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE (EAC PP) Version 1.3.2, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-12-05.

[BSI-CC-PP-0068-V2-2011-MA-01] Machine Readable Travel Document using Standard Inspection Procedure with PACE(PACE PP), BSI-CC-PP-0068-V2-2011-MA-01, Version 1.0.1, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014-07-22.

[BSI-CC-PP-0084-2014] Security IC Platform Protection Profile with Augmentation Packages, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.0, 2014-01-13.

[BSI-CC-PP-0086-2015] Common Criteria Protection Profile / Electronic document implementing Extended Access Control Version 2 defined in BSI TR-03110 [EAC2-PP], Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.01, 2015-05-20.

[BSI-TR-03110-1-V220] Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 1 - eMRTDs with BAC/PACEv2 and EACv1, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.20, 2015-02-26.

[BSI-TR-03110-2-V221] Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token ü Part 2 - Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.21, 2016-12-21.

[BSI-TR-03110-3-V221] BSI, Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3 - Common Specifications, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.21, 2016-12-21.

[BSI-TR-03110-4-V221] BSI, Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 4: Applications and Document Profiles, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.21, 21. December 2016

[BSI-TR-03111-V210-ECC] TR-03111, Technical Guideline TR-03111: Elliptic Curve Cryptography, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.10, 2018-06-01.

[BSI-TR-03116-2] TR-03116-2, Technische Richtlinie BSI TR-03116 - Kryptographische Verfahren für Projekte der Bundesregierung - Teil 2: Hoheitliche Dokumente, Bundesamt für Sicherheit in der Informationstechnik (BSI), Stand 2021, 2021-02-23.

[EU-Reg-910-2014] eIDAS Regulation (Regulation (EU) No 910/2014), REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Official Journal of the European Communities, L257:73 - 114, 2014-08-28.

[ICAO-9303-2015] ICAO Doc 9303, Machine Readable Travel Documents - Machine Readable Passports, (this includes the latest supplemental for ICAO Doc 9303 which also should be considered), International Civil Aviation Organization (ICAO), Seventh Edition, 2015.

[ICAO-TR-110] ICAO SAC v1.1, Machine Readable Travel Documents, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, International Civil Aviation Organization (ICAO), Version 1.1, 2014-04-15.

[NIST-FIPS-180-4] FIPS PUB 180-4, Secure Hash Standard (SHS), Information Technology Laboratory, National Institute of Standards and Technology (NIST), August 2015.

[NIST-FIPS-186-4] FIPS PUB 186-4, DIGITAL SIGNATURE STANDARD (DSS), Information Technology Laboratory, National Institute of Standards and Technology (NIST), 2013-07.

[NIST-FIPS-197] FIPS PUB 197, ADVANCED ENCRYPTION STANDARD (AES), Information Technology Laboratory, National Institute of Standards and Technology (NIST), 2001-11-26

[ISO-IEC-7816-part-2] ISO/IEC 7816: Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of contacts, Version Second Edition, ISO/IEC, 2008.

[ISO-IEC-7816-part-4] ISO/IEC 7816-4:2013, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange, ISO/IEC, 2013-04.

[ISO-IEC-14443-2018] ISO/IEC 14443 Identification cards – Contactless integrated circuit cards - Contactless proximity objects, ISO/IEC, 2018.

[ISO-IEC-9797-1-2011] ISO/IEC 9797-1:2011, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, ISO/IEC, 2011-03.

[RFC-5639-2010-03] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010-03.

[NIST-800-38A-2001] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, National Institute of Standards and Technology (NIST), 2001 Edition, 2001-12.

[NIST-SP800-67] NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, National Institute of Standards and Technology (NIST), Revision 2, 2012-01.

[NIST-SP800-90A] NIST Special Publication 800-90A, Recommendation Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology (NIST), Revision 1, 2015-06.

[RSA-PKCS1-v2.2] PKCS #1 v2.2: RSA Cryptography Standard, Version 2.2, 2012-10-27.

[RSA-PKCS-3-V1.4] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, 1993-11-01.

[Infineon-ST-SLC52-H13] Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h with Options, Common Criteria EAL6 augmented / EAL6+, Infineon, Version 1.9, 2021-05-18.

[Infineon-Chip-HW-Ref-16bit-V01] 16-bit Security Controller Family - V01, Hardware Reference Manual (HRM), Revision 7.0, 2019-06-11

[Infineon-Chip-HCL52] HCL52-CPU-C65 Hash Crypto Library for CPU SHA, 16-bit Security Controller, User interface manual, v1.12.001, 2020-01-14.

[ANSI-X9.62] American National Standard X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), ANSI, 2005-11-16.

[ANSI-X9.63] American National Standard X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, ANSI, 2001-11-20.

[ISO-IEC-14888-3] ISO/IEC 14888_3:2006 - Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms, ISO/IEC, 2006-11.

[ISO-IEC-11770-3] ISO/IEC 11770-3:2015, Information technology – Security techniques - Key management – Part 3: Mechanisms using asymmetric techniques, ISO/IEC, 2015-08.

[IEEE-1363] IEEE 1363A-2004, IEEE Standard Specifications for Public-Key Cryptography, IEEE Standards Board, 2004-07-22.

[SOG-IS-Crypto-Catalog-V1.2] SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms, Version 1.2, 2020-01.

[DIR-1999-93-EC] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures. Official Journal of the European Communities, L13:12 - 20, 2000-01-19.

[Atos-V60-ADM] Administrator Guidance ‘CardOS V6.0 ID R1.0’ and ‘CardOS V6.0 ID R1.0 (BAC)’, Atos Information Technology GmbH

[Atos-V60-USR] User Guidance ‘CardOS V6.0 ID R1.0’ and ‘CardOS V6.0 ID R1.0 (BAC)’, Atos Information Technology GmbH

Index