THALES
Building a future we can all trust

PPCA application on MultiApp V4.0.1 Platform Security Target Lite – Version 1.7p

Common Criteria / ISO 15408
Security Target – Public version
EAL5+

© Copyright Thales

TABLE OF CONTENTS

© Copyright Thales

TABLE OF FIGURES

© Copyright Thales

TABLE OF TABLES

© Copyright Thales

1. Reference documents

1.1. EXTERNAL REFERENCES [ER]

[ISO]	ISO references
[ISO14443]	Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Books 1 to 4
[Javacard]	**Javacard references**
[JCRE304]	Java Card 3.0.4 Runtime Environment (JCRE) Specification, Classic Edition – September 2011 – Published by Oracle
[JCVM304]	Java Card 3.0.4 Virtual Machine (JCVM) Specification, Classic Edition-– September 2011 – Published by Oracle
[JCAPI304]	Java Card 3.0.4 Application Programming Interface (API) Specification, Classic Edition-– September 2011 – Published by Oracle
[GP]	**Global Platform references**
[GP_22]	GlobalPlatform Card Specification Version 2.2.1, January 2011
[GP22_AmdD]	Secure Channel Protocol 03 – Global Platform Card Specification v2.2 – Amendment D Version 1.1, September 2009
[GP22_AmdE]	Security Upgrade for Card Content Management – Global Platform Card Specification v2.2 – Amendment E Version 1.0.1, July 2014
[GP22_ID]	Global Platform – ID Configuration v1.0
[TR03110]	**eIDAS Token specifications**
[TR03110-1]	Advanced Security Mechanisms for Machine Readable Travel Documents Part 1: eMRTDs with BAC/PACEv2 and EACv1 Version 2.20
[TR03110-2]	Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token Part 2: Protocols for electronic Identification, Authentication and trust Services Version 2.21
[TR03110-3]	Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token Part 3: Common Specifications Version 2.21
[TR03110-4]	Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token Part 4 : Applications and Document Profiles Version 2.21
[CC]	**Common Criteria references**
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[CCDB]	Common Criteria Supporting Document, Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices Ref: CCDB-2012-04-001, Version 1.2, April 2012.

[PP-JCS]	Java Card System Protection Profile – Open Configuration Ref: ANSSI-PP-2010-03M01, Version 3.0, May 2012
[PACEPP]	Common Criteria Protection Profile - Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) Ref: BSI-CC-PP-0068-V2-2011-MA-01
[PP-EAC2]	Common Criteria Protection Profile - Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110 [EAC2-PP] Ref: BSI-CC-PP-0086
[PP-0084]	Security IC Platform Protection Profile with augmentation Packages Ref: BSI-CC-PP-0084-2014
[ST_M7892]	Security Target Lite - M7892 Design Steps D11 and G12 Revision 3.6 as of 2021-08-05

1.2. INTERNAL REFERENCES [IR]

[AGD]	**TOE guidance documentation**
[REFMAN]	Polymorphic Pseudonym Card Application V1.0 - Reference Manual Ref: D1430671E, January 25th 2018
[AGD-TopLevel]	PPCA 1.0 application on MultiApp V4.0.1 Platform – AGD top-level document Ref: D1447007, Revision 1.3
[AGD_PLTF]	MultiApp ID Operating System Reference Manual Ref. : D1392687E
[Others]	**Other internal references**
[ST_PLT]	MultiApp V4.0.1 Javacard Platform - Security Target Ref: D1430789, Revision 1.3

2. Security Target introduction

2.1. SECURITY TARGET IDENTIFICATION

Title:	PPCA application on MultiApp V4.0.1 Platform – Security Target
Version:	1.7p
Author:	THALES
Reference:	D1432617
Publication date:	30/06/2022

2.2. TOE IDENTIFICATION

Product name:	MultiApp V4.0.1
TOE name:	PPCA application on MultiApp V4.0.1 Platform
TOE version:	1.0.1.3
TOE documentation:	Guidance [AGD]
TOE hardware part:	Infineon M7892 G12 security controller
Developer:	THALES

2.3. TOE OVERVIEW

The MultiApp V4.0.1 product addresses the identity market. Built upon an opened javacard platform, the application software implements identification and authentication services.

These services are enabled through the personalization of one or several corresponding applications:

- eTravel 2.2: MRTD application compatible with ICAO specifications
- PPCA 1.0: e-ID application providing pseudonym randomization services

Additionally, other applets – not determined at the moment of the present evaluation – may be loaded before or after issuance.

The product is a contactless smartcard compliant with [ISO14443], supporting T=CL Type A communication protocol.

© Copyright Thales

For the present evaluation, the Target of Evaluation (TOE) is the PPCA 1.0 applet and the underlying platform which supports its functionality. Therefore, the TOE boundaries encompass:

- **The PPCA application software made of the following parts:**
  - The PPCA Applet Software
  - The MultiApp V4.0.1 javacard platform, based on [Javacard] and [GP], which supports the execution of the personalized applets and provides card administration services
- **The associated smart card data, made of :**
  - The PPCA applet data
  - The data stored by the MultiApp V4.0.1 javacard platform (card-related data)
- **The M7892 G12 Integrated Circuit**
- **The guidance documentation [AGD]**

Note 1: only the parts and features of the MultiApp V4.0.1 javacard platform, which support the installation and execution of the PPCA applet, are within the TOE scope. Other javacard platform parts and features are out of the TOE.

Note 2: as mentioned above, other applets may also be embedded in the MultiApp V4.0.1 product, but are not in the TOE scope for the present evaluation.

Note 3: the product includes a plastic body or inlay, and associated security elements (such as holograms, security printing…) which are also outside the TOE scope.

© Copyright Thales

3. TOE Description

3.1. ARCHITECTURE OF THE MULTIAPP V4.0.1 PRODUCT

The high-level architecture of the MultiApp V4.0.1 product can be represented by Figure 1.

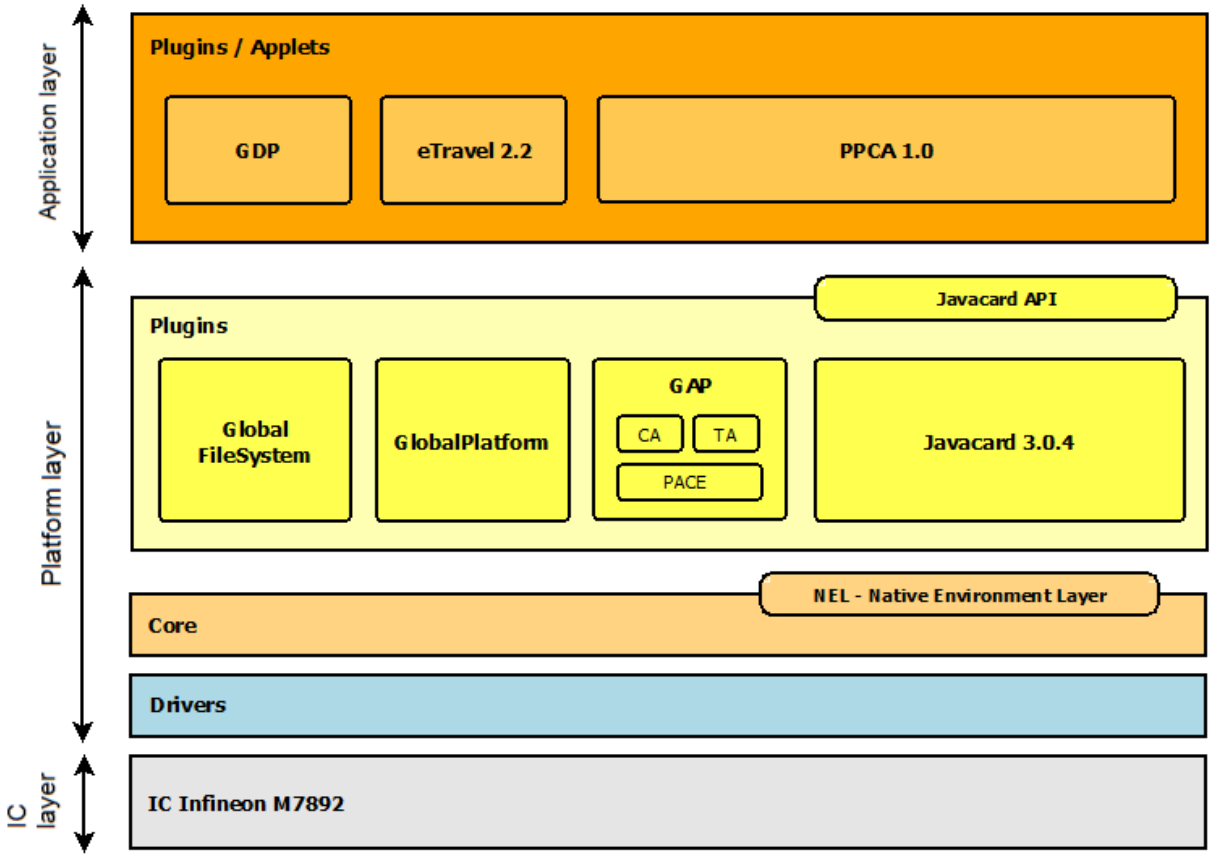

Figure 1: MultiApp V4.0.1 product architecture

The architecture can be decomposed in three layers:

- The hardware layer composed of the M7892 G12 integrated circuit
- The MultiApp V4.0.1 platform, which is the operating system of the product
- The application layer, encompassing all the product applications.

MultiApp V4.0.1 is a flash product, therefore the platform and applications executable code is stored in flash code area. All the data are located in flash data area. The separation between these data is ensured by the javacard firewall as specified in [JCRE304].

3.2. TOE BOUNDARIES

The TOE physical boundaries encompass the M7892 IC containing the Thales embedded software (MultiApp V4.0.1 platform and applets on top of it). Note that the product also includes a plastic body and associated elements (such as antenna, security printing…) but these are outside the TOE physical boundary.

As highlighted by Figure 2, the TOE logical boundaries encompass:

- The PPCA application
- The GDP applet for personalization
- The MultiApp V4.0.1 Javacard Platform
- The underlying M7892 Integrated Circuit

The [AGD] documentation is also part of the TOE.

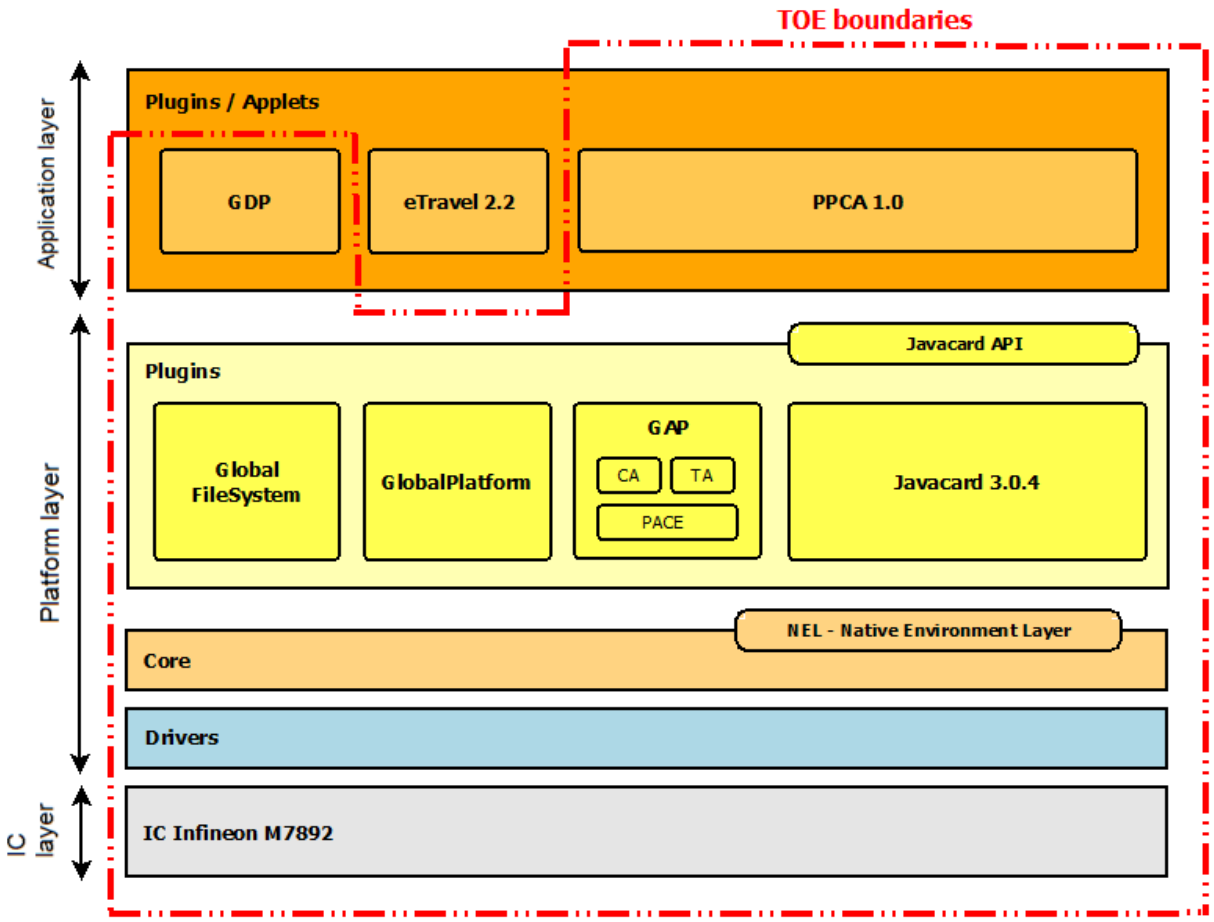

Figure 2: TOE logical boundaries

3.3. MULTIAPP V4.0.1 PLATFORM DESCRIPTION

The MultiApp V4.0.1 platform is an operating system that complies with major industry standards:

- Oracle's Java Card 3.0.4, which consists of the Java Card 3.0.4 Virtual Machine [JVCM304], the Java Card 3.0.4 Runtime Environment [JCRE304] and the Java Card 3.0.4 Application Programming Interface [JCAPI304].
- The Global Platform Card Specification version 2.2.1 [GP22]
- GAP: the General Authentication Procedure, for compliance with latest version of [TR03110]

The MultiApp V4.0.1 platform provides the following services:

- Initialization of the Card Manager and management of the card life cycle
- Secure loading and installation of the applets under Security Domain control
- Deletion of applications under Security Domain control
- Extradition services to allow several applications to share a dedicated Security Domain
- Secure channel according to GP [GP22] and PACE protocols.
- Secure operation of the applications through the API
- Management and control of the communication between the card and the CAD
- Application life cycle management
- Card basic security services as follows:
    - Checking environmental operating conditions using information provided by the IC
    - Checking life cycle consistency
    - Ensuring the security of the PIN and cryptographic key objects
    - Generating random numbers
    - Handling secure data object and backup mechanisms
    - Managing memory content
    - Ensuring Java Card firewall mechanism

GAP and File System APIs are required for the [TR03110] based applications.

GDP stands for Global Dispatcher Perso application. It centralizes application personalization (at first for eTravel).

Support of Flash Modularity: it is possible, during product construction, to embed only features required for a given customer.

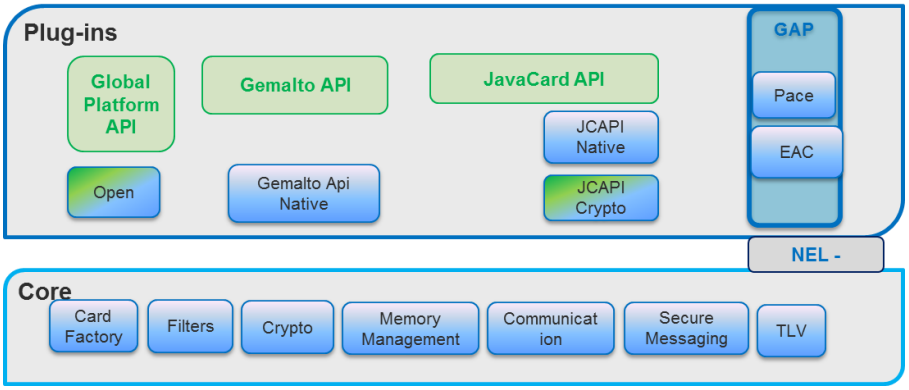

Figure 3: MultiApp V4.0.1 Java Card platform architecture

The Core layer

It provides the basic card functionalities (memory management, I/O management and cryptographic primitives) with native interface with the underlying IC. In-house cryptographic libraries are used and are implemented in the native layer, encompassing the following algorithms:

- DES, 3DES (ECB, CBC)
- RSA up to 4096 (CRT method & public Std method), 2048 (Std private method)
- DH up to 2048
- AES 128, 192, 256
- SHA1, SHA 2 (224, 256, 384, 512)
- HMAC based on SHA1 and SHA2 (224, 256, 384, 512)
- ECC (ECDSA et ECDH) up to 521
- PACE DH up to 2048 Integrated Mapping, Generic Mapping
- PACE ECDH up to 521 Integrated Mapping, Generic Mapping
- Pseudo-Random Number Generation (PRNG) & Software random.
- Pseudonymous signature (Psign) ECC up to 521

The **Javacard Runtime Environment**

It conforms to [JCRE304] and provides a secure framework for the execution of the Java Card programs and data access management (firewall).

Among other features, multiple logical channels are supported, as well as extradition, DAP, Delegated management, SCP01, SCP02 and SCP03.

The **Javacard Virtual Machine**

It conforms to [JVCM304] and provides the secure interpretation of bytecodes.

The **API**

It includes the standard Java Card API [JCAPI304] and the Thales proprietary API.

The **Global Platform Issuer Security Domain**

It conforms to [GP22] and provides card, key and applet management functions (contents and life-cycle), GP secure channel and security control.

The **GAP component**

GAP is an extension of PACE, it provides additional commands terminal authenticate (TA) and Chip Authenticate (CA). This provides mutual authentication, secure messaging channel, authorization verified by application through specific API.

3.4. PPCA APPLICATION DESCRIPTION

The Dutch government intends to issue an electronic driving license with a chip that contains a PPCA applet besides the eTravel application.

The eTravel applet needs to comply with the European Regulation (EU) 383/2012. The PPCA applet needs to be able to fulfill the role of authentication means at assurance level 'high' according to the eIDAS Regulation (EU) 910/2014 and needs to comply with specific requirements for the Dutch scheme. It complies with BSI TR 3110 v 2.21 part 2, 3 and 4.

3.5. TOE LIFE-CYCLE

The product and TOE life cycle is composed of 7 phases which are described in table 1. The table also mentions the actor(s) involved in each phase, as well as the associated location(s).

The IC does not contain any part of the MultiApp V4.0.1 software prior to phase 5. The loading of the MultiApp V4.0.1 software occurs during phase 5, after which the IC loading service is locked and no more available.

As described, at the end of phase 5 Thales delivers pre-personalized MultiApp V4.0.1 cards to an accredited Personalizer. At this stage, the TOE is entirely built and protects itself through the security mechanisms implemented in the operating system and the underlying IC. Consequently, the TOE delivery point - which determines the boundary between the ALC and AGD Common Criteria assurance classes - is put at the end of phase 5, as illustrated in figure 5.

Note: The guidance documentation [AGD] is delivered in the form of electronic documents (pdf format) by the Thales technical representative:

- At the end of phase 5 to the Personalizer
- On demand to the Card Issuer

Phase	Designation	Description / comments		Actor	Location
1	Embedded Software (ES) development	MultiApp V4.0.1 platform development	Platform development & tests	**Thales** GP R&D team - secure environment -	**Thales Singapore** site
				Thales SL Crypto team - secure environment -	**Thales Meudon** site
		PPCA applet development	Applet development & tests	**Thales** GP R&D team - secure environment -	**Thales Vantaa** site
		CC evaluation	Common Criteria activities	**Thales** CC team - secure environment -	**Thales La Ciotat** site
		Industrialization	Management of the delivery process between Thales and Infineon	**Thales** Component group - secure environment -	**Thales Gémenos** site
			Production scripts development for phases 4 and 5 (assembly, preperso). Delivery to the production sites.	**Thales** PSE team - secure environment -	**Thales Gémenos** site **Thales Singapore** site
2	IC development	Development of the M7892 security controller and associated tools		**Infineon** - Secure environment -	Infineon site(s) as stated in the M7892 CC certificate
3	IC manufacturing	Manufacturing of virgin M7892 integrated circuits embedding the Infineon flash loader, and protected by a dedicated Thales key.		**Infineon** - Secure environment -	Infineon site(s) as stated in the M7892 CC certificate
4	Module manufacturing	IC packaging & testing		**Thales** - Secure environment -	**Thales Gémenos** site **Thales Singapore** site **Thales Curitiba** site
5	Card manufacturing and pre-personalization	Module embedding in plastic card body Loading of the MultiApp V4.0.1 software (platform and pre-issuance applications) Preperso and Testing		**Thales** - Secure environment -	**Thales Gémenos** site **Thales Tczew** site **Thales Vantaa** site **Thales Singapore** site **Thales Curitiba** site
6	Card personalization	Creation of files and loading of end-user data.		**Accredited Personalizer** - Secure environment -	
7	End-usage	End-usage for issuer and cardholder		Card issuer and end-user	Field

Table 1: Product and TOE life-cycle phases

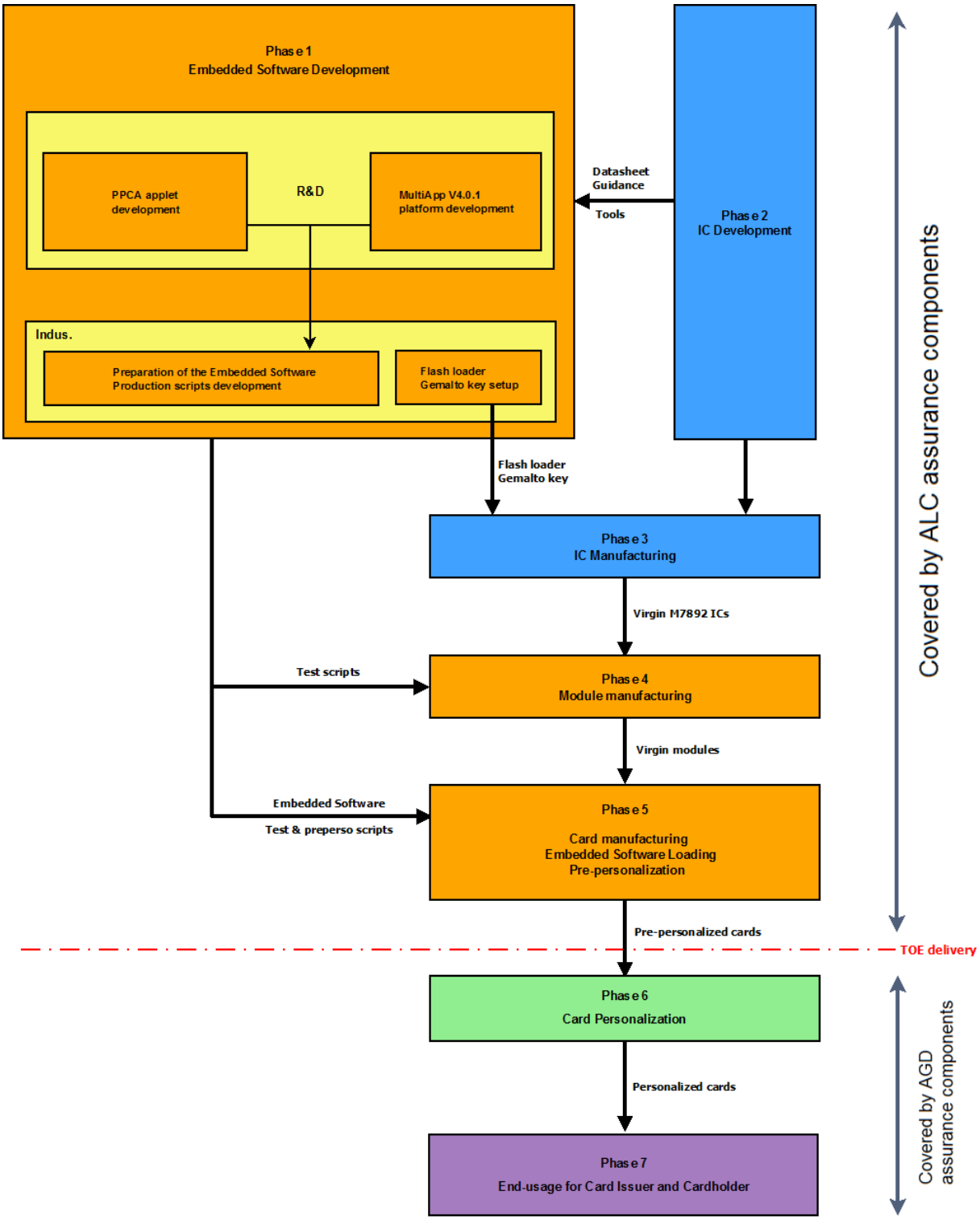

Figure 4: Product and TOE life-cycle

3.6. TOE USERS

The TOE users (in the CC meaning, i.e. after TOE delivery) are described hereunder:

Personalizer

The Personalizer personalizes the card by loading the cardholder data as well as cryptographic keys and PIN. At the end of this phase, the card is in OP_SECURED state.

Card Issuer, Administrator

The Card Issuer -short named “issuer”- is a governmental administration. It issues cards to the citizens who are the “Card holders”. The Card Issuer has also the role of Administrator. Therefore, the Card Issuer is responsible for selecting and managing the personalization, for managing applets, and for distribution and invalidation of the card.

End-user

The End-user holds the TOE in the usage phase (phase 7). The card is personalized with his or her identification and secrets. His uses the TOE to access government services.

4. Conformance claims

Common criteria Version: This ST conforms to CC Version 3.1 [CC-1] [CC-2] [CC-3]

Conformance to CC part 2 and 3:

- This ST is CC part 2 extended with the FCS_RND.1, FAU_SAS.1, FMT_LIM.1, FMT_LIM.2, FPT_EMS.1 and FIA_API.1 families. All the other SFRs have been drawn from the catalogue of requirements in CC part 2 [CC-2].
- This ST is CC part 3 conformant. It means that all SARs in that ST are based only upon assurance components in CC part 3 [CC-3].

Assurance package conformance: EAL4 augmented (EAL4+)
This ST conforms to the assurance package EAL4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

Evaluation type: this is a composite evaluation, which relies on the MultiApp V4.0.1 platform certificate and evaluation results.

MultiApp V4.0.1 platform certificate:

- Certification done under the ANSSI scheme
- Certification report ANSSI-CC-2017/76
- Security Target [ST_PLT] conformant to Javacard Protection Profile, Open configuration [PP-JCS]
- Common criteria version: 3.1
- Assurance level: EAL5+ (ALC_DVS.2 and AVA_VAN.5 augmentations)

Consequently, the present evaluation includes the additional composition tasks defined in the CC supporting document “Composite product evaluation for smart cards and similar devices” [CCDB].

Note: the MultiApp V4.0.1 platform was also evaluated in composition with the M7892 G12 integrated circuit, and relied upon on the chip certificate and evaluation results:

M7892 G12 chip certificate:

- Certification done under the BSI scheme
- Certification report BSI-DSZ-CC-0891-V2-2016
- Security Target [ST_M7892] strictly conformant to IC Protection Profile [PP-0084]
- Common criteria version: 3.1
- Assurance level: EAL6+ (ALC_FLR.1, ALC_DVS.2 and AVA_VAN.5 augmentations)

Protection Profile (PP): this Security Target is based on the [PP-EAC2] protection profile. PP conformance is not claimed as the TOE doesn’t implement the Restricted Identification (RI) protocol, therefore the following items had to be removed:

- P.RestrictedIdentity

- OT.RI_EAC2
- OE.RestrictedIdentity
- FIA_API.1/RI

All other elements from [PP-EAC2] have been kept identical.

5. Security problem definition

5.1. ASSETS

The following assets are listed in [PP-EAC2] and shall be considered for the present evaluation.

5.1.1. Primary assets

Authenticity of the Electronic Document's Chip	The authenticity of the electronic document's chip, personalized by the issuing state or organization for the electronic document holder, is used by the electronic document presenter to prove his possession of a genuine electronic document. Generic Security Property: Authenticity This asset is equal to the one defined in [PACEPP].
Tracing Data	Technical information about the current and previous locations of the electronic document gathered unnoticeable by the electronic document holder recognizing the TOE not knowing any PACE password. TOE tracing data can be provided / gathered. Generic Security Property: Unavailability This asset is equal to the one defined in [PACEPP]. Note that unavailability here is required for anonymity of the electronic document holder.
Sensitive User Data	User data, which have been classified as sensitive data by the electronic document issuer, e. g. sensitive biometric data. Sensitive user data are a subset of all user data, and are protected by EAC2. Generic Security Properties: Confidentiality, Integrity, Authenticity
User Data stored on the TOE	All data, with the exception of authentication data, that are stored in the context of the application(s) on the electronic document. These data are allowed to be accessed either by a PACE terminal, or, in the case of sensitive data, by an EAC2 terminal with appropriate authorization level. Generic Security Properties: Confidentiality, Integrity, Authenticity This asset is an extension of the asset defined in [PACEPP].
User Data transferred between the TOE and the Terminal	All data, with the exception of authentication data, that are transferred (both directions) during usage of the application(s) of the electronic document between the TOE and authenticated terminals. Generic Security Properties: Confidentiality, Integrity, Authenticity This asset is an extension of the asset defined in [PACEPP]. As for confidentiality, note that even though not each transferred data element represents a secret, [TR03110-2] requires confidentiality of all transferred data by secure messaging, employing the encrypt-then-authenticate approach.

All the primary assets represent user data in the sense of Common Criteria (CC).

5.1.2. Secondary assets

Accessibility of TOE Functions and Data only for Authorized Subjects	Property of the TOE to restrict access to TSF and TSF-Data stored in the TOE to authorized subjects only. Generic Security Property: Availability
Genuineness of the TOE	Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. Generic Security Property: Availability
Electronic Document Communication Establishment Authorization Data	Restricted-revealable authorization information for a human user used for verification of the authorization attempts as an authorized user (PACE password). These data are stored in the TOE and not send to it. Restricted-revealable here refers to the fact that if necessary, the electronic document holder may reveal her verification values of CAN and MRZ to an authorized person, or to a device that acts according to respective regulations and is considered trustworthy. Generic Security Properties: Confidentiality, Integrity
Secret Electronic Document Holder Authentication Data	Secret authentication information for the electronic document holder being used for verification of the authentication attempts as authorized electronic document holder (sent PACE passwords, e.g. PIN or CAN). Generic Security Properties: Confidentiality, Integrity
TOE internal Non-Secret Cryptographic Material	Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material used by the TOE in order to enforce its security functionality. An example for such non-secret material is the document security object (SOD) that contains a digital signature. Generic Security Properties: Integrity, Authenticity
TOE internal Secret Cryptographic Keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality. Generic Security Properties: Confidentiality, Integrity

Application Note 2: Data for electronic document holder authentication and for authorization of communication with the electronic document can be categorized as (i) reference information that are persistently stored within the TOE, and (ii) verification information for the TOE that are input by a human user during an authentication and/or authorization attempt. The TOE shall secure both reference information, and, together with the connected terminal, verification information that are transferred in the channel between the TOE and the terminal.

Application Note 3: The above secondary assets represent TSF and TSF-Data in the sense of CC.

5.2. SUBJECTS

The following subjects are listed in [PP-EAC2] and shall be considered for the present evaluation:

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 that have to be maintained. The attacker is assumed to possess at most high attack potential. Note that the attacker might capture any subject role recognized by the TOE.
Country Signing Certification Authority (CSCA)	An organization enforcing the policy of the electronic document issuer, i. e. confirming correctness of user and TSF data that are stored within the electronic document. The CSCA represents the country specific root of the public key infrastructure (PKI) for the electronic document, and creates Document Signer Certificates within this PKI. The CSCA also issues a self-signed CSCA certificate that has to be distributed to other countries by secure diplomatic means, see [ICAO9303].
Country Verifying Certification Authority (CVCA)	The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing state or organization, i. e. enforcing protection of sensitive user data that are stored in the electronic document. The CVCA represents the country specific root of the PKI of EAC2 terminals, and creates Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed as CVCA Link-Certificates, see [TR03110-3].
Document Signer (DS)	An organization enforcing the policy of the CSCA. A DS signs the Document Security Object (SOD) that is stored on the electronic document for Passive Authentication. A Document Signer is authorized by the national CSCA that issues Document Signer Certificates, see [ICAO9303]. Note that this role is usually delegated to a Personalization Agent.
Document Verifier (DV)	An organization issuing terminal certificates. The DV is a Certificate Authority, authorized by the corresponding CVCA to issue certificates for EAC2 terminals, see [TR03110-3].
Electronic Document Holder	A person who the electronic document issuer has personalized the electronic document for. Personalization here refers to associating a person uniquely with a specific electronic document. Note that an electronic document holder can also be an attacker.
Electronic Document Presenter	A person presenting the electronic document to a terminal and claiming the identity of the electronic document holder. Note that an electronic document presenter can also be an attacker, cf. below.
Manufacturer	Generic term comprising both the IC manufacturer that produces the integrated circuit, and the electronic document manufacturer that creates the electronic document and attaches the IC to it. The manufacturer is the default user of the TOE during the manufacturing life cycle phase. When referring to the role manufacturer, the TOE itself does not distinguish between the IC manufacturer and the electronic document manufacturer.
PACE Terminal	A PACE terminal implements the terminal part of the PACE protocol, and authenticates itself to the electronic document using a shared password (CAN, PIN, PUK or MRZ). A PACE terminal is not allowed to access sensitive user data.
Personalization Agent	An organization acting on behalf of the electronic document issuer that personalizes the electronic document for the electronic document holder. Personalization includes some or all of the following activities: (i) establishing the identity of the electronic document holder for the biographic data in the electronic document, (ii) enrolling the biometric reference data of the electronic document holder, (iii) writing a subset of these data on the physical electronic document (optical personalization) and storing them within the electronic document's chip (electronic personalization), (iv) writing document meta data (i. e. document type, issuing country, expiry date, etc.) (v) writing the initial TSF data, and (vi) signing the Document Security Object , and the elementary files EF.CardSecurity and the EF.ChipSecurity (if applicable [ICAO9303], [TR03110-3]) in the role DS. Note that the role personalization agent may be distributed among several institutions according to the operational policy of the electronic document issuer.
EAC2 Terminal	A terminal that has successfully passed Terminal Authentication 2 is an EAC2 terminal. It is authorized by the electronic document issuer through the Document Verifier of the receiving branch (by issuing terminal certificates) to

	access a subset or all of the data stored on the electronic document.
Terminal	A terminal is any technical system communicating with the TOE through the contactless or contact-based interface. The role terminal is the default role for any terminal being recognized by the TOE that is neither a PACE terminal nor anEAC2 terminal.

5.3. THREATS

5.3.1. EAC2 Protection Profile

The following threats are listed specifically in the [PP-EAC2] and shall be considered for the present evaluation.

T.Counterfeit/EAC2	Counterfeit of electronic document chip data Adverse action: an attacker with high attack potential produces an unauthorized copy or reproduction of a chip of a genuine electronic document. This copy or reproduction can be used as a part of a counterfeit electronic document. This violates the authenticity of the electronic document's chip used for authentication of an electronic document presenter by possession of an electronic document. The attacker may generate a new data set or extract completely or partially the data from a genuine electronic document's chip and copy them to another appropriate chip to imitate the chip of the genuine electronic document. Threat agent: having high attack potential, being in possession of one or more legitimate ID-Cards Asset: authenticity of user data stored on the TOE
T.Sensitive_Data	Unauthorized access to sensitive user data Adverse action: an attacker tries to gain access to sensitive user data through the communication interface of the electronic document's chip. The attack T.Sensitive_Data is similar to the threat T.Skimming from [PACEPP] w.r.t. the attack path (communication interface) and the motivation (to get data stored on the electronic document's chip) but differs from those in the asset under the attack (sensitive data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods. Threat agent: having high attack potential, knowing the PACE Password, being in possession of a legitimate electronic document Asset: confidentiality of sensitive user data stored on the electronic document

5.3.2. PACE Protection Profile

According to [PP-EAC2], the following threats listed in [PACEPP] shall also be considered for the present evaluation.

T.Abuse-Func	Abuse of Functionality 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 initialization and personalization 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
T.Eavesdropping	Eavesdropping on the communication between the TOE and the PACE terminal 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
T.Forgery	Forgery of Data 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 the PACE authenticated BIS-PACE 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 Application Note 4: T.Forgery from [PACEPP] is extended here to all kinds of (PACE terminals and EAC2 terminals) targets that are outsmarted by the attacker.
T.Information_Leakage	Information Leakage from travel document 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 Application Note 5: Confidential user data in T.Information_Leakage from [PACEPP] include sensitive user data defined in this PP.
T.Malfunction	Malfunction due to Environmental Stress 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.
T.Phys-Tamper	Physical Tampering 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), (ii) 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.
T.Skimming	Skimming travel document / Capturing Card-Terminal Communication 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
T.Tracing	Tracing travel document 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

5.4. ORGANISATIONAL SECURITY POLICIES

5.4.1. EAC2 Protection Profile

The following OSP are listed specifically in [PP-EAC2] and shall be considered for the present evaluation.

P.EAC2_Terminal	Abilities of Terminals executing EAC Version 2 Terminals that intent to be EAC2 terminals must implement the respective terminal part of the protocols required to execute EAC version 2 according to [TR03110-2], and store (static keys) or generate (temporary keys and nonces)

	the corresponding credentials.
P.Terminal_PKI	PKI for Terminal Authentication The electronic document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the electronic document issuer shall run a Country Verifying Certification Authority. The instances of the PKI shall fulfill the requirements and rules of the corresponding certificate policy. The electronic document issuer shall make the CVCA certificate available to the personalization agent or the manufacturer.

5.4.2. PACE Protection Profile

According to [PP-EAC2], the following OSP listed in [PACEPP] shall also be considered for the present evaluation.

P.Card_PKI	PKI for Passive Authentication (issuing branch) 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 (CCSCA). 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 (CCSCA) having to be made available to the travel document Issuer by strictly secure means, see [6], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer, see [6], 5.5.1. 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.
P.Manufact	Manufacturing of the travel document's chip The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The travel document Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.
P.Pre-Operational	Pre-operational handling of the travel document 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. 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. 4.) If the travel document Issuer authorizes a Personalization Agent to personalize the travel document for travel document holders, the travel document Issuer has to ensure that the Personalization Agent acts in

	accordance with the travel document Issuer's policy.
P.Terminal	Abilities and trustworthiness of terminals 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 [6]. 2.) They shall implement the terminal parts of the PACE protocol [4], of the Passive Authentication [6] and use them in this order. 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 of CCSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [6]). 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.
P.Trustworthy_PKI	Trustworthiness of PKI The CSCA shall ensure that it issues its certificates exclusively to the rightful organizations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the travel document.

5.5. SECURE USAGE ASSUMPTIONS

5.5.1. EAC2 Protection Profile

According to [PP-EAC2], the following assumption listed in [PACEPP] shall be considered for the present evaluation.

A.Passive_Auth	PKI for Passive Authentication The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document. The issuing State or Organization 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 Organizations. It is assumed that the Personalization Agent ensures that the Document Security Object contains only the hash values of genuine user data according to [6].

5.5.2. JCS Protection Profile

The following assumptions, derived from [PP-JCS], shall also be considered for the present evaluation, in order to address concerns related to post-issuance loading of applications.

A.APPLET	Applets loaded post-issuance do not contain native methods. The Java Card specification [JCVM222] §3.3 explicitly mentions "does not include support for native methods" outside the API.
A.VERIFICATION	All the bytecodes are verified at least once before the loading, in order to ensure that each bytecode is valid at execution time.
A.CODE-EVIDENCE	For application code loaded during the Personalization phase (Phase 6), organizational measures or evaluated technical measures implemented by the TOE ensure that the loaded application has not been changed since the code verifications mentioned in A.VERIFICATION. For application code loaded post-issuance and verified off-card according to A.VERIFICATION, the verification authority provides digital evidence to the TOE that the application code has not been modified after the code verification and that he is the actor who performed code verification.

5.6. COMPOSITION TASKS – SECURITY PROBLEM DEFINITION PART

5.6.1. Statement of Compatibility – Threats part

The following table (see next page) lists the relevant threats of the security target [ST_PLT], and provides the link to the threats on the composite-product, showing that there is no contradiction between the two.

Platform relevant threat label	Platform relevant threat content	Link to the composite-product threats
T.CONFID-APPLI-DATA	The attacker executes an application to disclose data belonging to another application.	T.Counterfeit/EAC2 T.Sensitive_Data
T.CONFID-JCS-CODE	The attacker executes an application to disclose the Java Card System code.	T.Counterfeit/EAC2 T.Sensitive_Data T.Forgery
T.CONFID-JCS-DATA	The attacker executes an application to disclose data belonging to the Java Card System.	T.Counterfeit/EAC2
T.INTEG-APPLI-CODE	The attacker executes an application to alter (part of) its own code or another application's code.	T.Forgery
T.INTEG-APPLI-CODE.LOAD	The attacker modifies (part of) its own or another application code when an application package is transmitted to the card for installation.	T.Forgery
T.INTEG-APPLI-DATA	The attacker executes an application to alter (part of) another application's data.	T.Forgery
T.INTEG-APPLI-DATA.LOAD	The attacker modifies (part of) the initialization data contained in an application package when the package is transmitted to the card for installation.	T.Forgery
T.INTEG-JCS-CODE	The attacker executes an application to alter (part of) the Java Card System code.	T.Forgery T.Counterfeit/EAC2 T.Sensitive_Data T.Information_Leakage
T.INTEG-JCS-DATA	The attacker executes an application to alter (part of) Java Card System or API data.	T.Forgery T.Counterfeit/EAC2 T.Sensitive_Data
T.SID.1	An applet impersonates another application, or even the Java Card RE, in order to gain illegal access to some resources of the card or with respect to the end user or the terminal.	T.Counterfeit/EAC2 T.Sensitive_Data
T.SID.2	The attacker modifies the TOE's attribution of a privileged role (e.g. default applet and currently selected applet), which allows illegal impersonation of this role.	T.Counterfeit/EAC2 T.Sensitive_Data
T.EXE-CODE.1	An applet performs an unauthorized execution of a method.	T.Counterfeit/EAC2 T.Sensitive_Data T.Forgery
T.EXE-CODE.2	An applet performs an execution of a method fragment or arbitrary data.	T.Counterfeit/EAC2 T.Sensitive_Data T.Forgery
T.NATIVE	An applet executes a native method to bypass a security function such as the firewall.	T.Counterfeit/EAC2 T.Sensitive_Data T.Forgery
T.RESOURCES	An attacker prevents correct operation of the Java Card System through consumption of some resources of the card: RAM or NVRAM.	No direct link to the composite-product threats, but no contradiction with them
T.DELETION	The attacker deletes an applet or a package already in use on the card, or uses the deletion functions to	No direct link to the composite-product

Platform relevant threat label	Platform relevant threat content	Link to the composite-product threats
	pave the way for further attacks (putting the TOE in an insecure state).	threats, but no contradiction with them
T.INSTALL	The attacker fraudulently installs post-issuance of an applet on the card. This concerns either the installation of an unverified applet or an attempt to induce a malfunction in the TOE through the installation process.	T.Counterfeit/EAC2 T.Sensitive_Data T.Forgery
T.OBJ-DELETION	The attacker keeps a reference to a garbage collected object in order to force the TOE to execute an unavailable method, to make it to crash, or to gain access to a memory containing data that is now being used by another application.	T.Counterfeit/EAC2 T.Sensitive_Data T.Forgery
T.PHYSICAL	The attacker discloses or modifies the design of the TOE, its sensitive data or application code by physical (opposed to logical) tampering means. This threat includes IC failure analysis, electrical probing, unexpected tearing, and DPA. That also includes the modification of the runtime execution of Java Card System or SCP software through alteration of the intended execution order of (set of) instructions through physical tampering techniques.	T.Information_Leakage T.Phys-Tamper
T.Skimming	Capturing Card-Terminal Communication: an attacker imitates a PACE terminal (e.g. inspection system) in order to get access to the user data stored on or transferred between the TOE and the use (e.g. inspecting authority) connected via the contactless/contact interface of the TOE.	T.Skimming
T.Eavesdropping	Eavesdropping on the communication between the TOE and the PACE terminal: an attacker is listening to the communication between the TOE (e.g. travel document) and the PACE authenticated terminal (e.g. BIS-PACE) in order to gain the user data transferred between the TOE and the terminal connected.	T.Eavesdropping
T.Abuse-Func	Abuse of Functionality: 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 initialization and personalization in the operational phase after delivery to the Application user.	T.Abuse-Func
T.Information_Leakage	Information Leakage from travel document: 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 TOE and associated applications (e.g. 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.	T.Information_Leakage
T.Phys-Tamper	Physical Tampering: an attacker may perform physical probing of the TOE and associated applications (e.g. 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 TOE and associated applications (e.g. travel document) in order to alter (I) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the TOE and associated application data (e.g. travel document).	T.Phys-Tamper
T.Malfunction	Malfunction due to Environmental Stress: An attacker may cause a malfunction the TOE (hardware and software) and associated applications by applying environmental stress in order to (i) deactivate or modify	T.Malfunction

Platform relevant threat label	Platform relevant threat content	Link to the composite-product threats
	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 TOE and associated applications (e.g. travel document) outside the normal operating conditions, exploiting errors in the TOE and associated applications (e.g. travel document) Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.	
T.Forgery	Forgery of Data: an attacker fraudulently alters the User Data or/and TSF-data stored on Toe or associated application (e.g. the travel document) or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated terminal (e.g. BIS-PACE by means of changed Application user data. The attacker does it in such a way that the terminal connected perceives these modified data as authentic one	T.Forgery

© Copyright Thales

5.6.2. *Statement of compatibility – OSPs part*

The following table lists the relevant OSPs of the security target [ST_PLT], and provides the link to the OSPs related to the composite-product, showing that there is no contradiction between the two.

Platform OSP label	Platform OSP content	Link to the composite product
OSP. VERIFICATION	This policy shall ensure the consistency between the export files used in the verification and those used for installing the verified file. The policy must also ensure that no modification of the file is performed in between its verification and the signing by the verification authority. If the application development guidance provided by the platform developer contains recommendations related to the isolation property of the platform, this policy shall also ensure that the verification authority checks that these recommendations are applied in the application code.	Covered by ALC audited processes in case of pre-issuance loading. Covered by OE.CODE-EVIDENCE in case of post-issuance loading.
OSP.SpecificAPI	The TOE must contribute to ensure that application can optimize control on its sensitive operations using a dedicated API provided by TOE. TOE will provide services for secure array management and to detect loss of data integrity and inconsistent execution flow and react against tearing or fault induction.	Used by the composite-product to strengthen PPCA applet security.
OSP.RND	This policy shall ensure the entropy of the random numbers provided by the TOE to applet using [JCAPI304] is sufficient. Thus attacker is not able to predict or obtain information on generated numbers.	This OSP at platform level directly supports the security of the authentication processes enforced within the composite-product (e.g. for the generation of keys or challenges).
P.Terminal	Abilities and trustworthiness of terminals: the Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows […]	P.Terminal
P.Personalisation	Personalization of the applicative data by authorized issuing actor only: the issuer guarantees the correctness of the user data to be included in TOE in Personalization phase. In particular, the issuer guarantees user data are consistent with respect of the end user of the TOE.	P.Pre-Operational
P.Manufact	Manufacturing of the TOE with Initialization Data for application: the Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.	P.Manufact
P.Pre-Operational	Pre-operational handling of the TOE and associated applications: […]	P.Pre-Operational

5.6.3. *Statement of compatibility – Assumptions part*

The following table (see next page) lists the relevant assumptions of the security target [ST_PLT], and provides the link to the assumptions related to the composite-product, showing that there is no contradiction between the two.

Platform assumption label	Platform assumption content	IrPA	CfPA	SgPA	Link to the composite product
A.APPLET	Applets loaded post-issuance do not contain native methods. The Java Card specification explicitly "does not include support for native methods" ([JCVM222], §3.3) outside the API.			**X**	A.APPLET
A.VERIFICATION	All the bytecodes are verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time.		**X**	**X**	• During phases 1, 4 and 5: CfPA Fulfilled by the ALC composite-SARs and the audit of pre-issuance verification processes. • During phases 6 and 7: SgPA A.VERIFICATION
A.Insp_Sys	Inspection Systems for global interoperability: the Extended Inspection System (EIS) for global interoperability (i) implements at least the terminal part of PACE [ICAO-TR-SAC]. If several protocols are supported by the EIS, PACE secure channel must be established and applicative data (e.g. the logical travel document) must be transferred under PACE. Other operations may be done when additional protocols are supported by the terminal.			**X**	P.Terminal

© Copyright Thales

6. Security objectives

6.1. SECURITY OBJECTIVES FOR THE TOE

6.1.1. EAC2 Protection Profile

The following TOE security objectives are listed in [PP-EAC2] and shall be considered for the present evaluation.

OT.AC_Pers_EAC2	Personalization of the Electronic Document The TOE must ensure that user data and TSF-Data that are permanently stored in the TOE can be written by authorized personalization agents only, with the following exception: An EAC2 terminal may also write or modify user data according to its effective access rights. The access rights are determined by the electronic document during Terminal Authentication 2. Justification: This security objective for the TOE modifies OT.AC_Pers from [PACEPP] as the additional features of EAC2 allow a strongly controlled, secure and fine-grained access to individual data groups of the electronic document.
OT.CA2	Proof of the Electronic Document's Chip Authenticity The TOE must allow EAC2 terminals to verify the identity and authenticity of the electronic document's chip as being issued by the identified issuing state or organization by Chip Authentication 2 [TR03110-2]. The authenticity of the chip and its proof mechanism provided by the electronic document's chip shall be protected against attacks with high attack potential.
OT.Sens_Data_EAC2	Confidentiality of sensitive User Data The TOE must ensure confidentiality of sensitive user data by granting access to sensitive data only to EAC2 terminals with corresponding access rights. The authorization of an EAC2 terminal is the minimum set of the access rights drawn from the terminal certificate used for successful authentication and the corresponding DV and CVCA certificates, and the access rights sent to the electronic document as part of PACE. The TOE must ensure confidentiality of all user data during transmission to an EAC2 terminal after Chip Authentication 2. Confidentiality of sensitive user data shall be protected against attacks with high attack potential.

6.1.2. PACE Protection Profile

According to [PP-EAC2], the following TOE security objectives listed in [PACEPP] shall also be considered for the present evaluation.

OT.Data_Authenticity	Authenticity of Data The TOE must ensure authenticity of the User Data and the TSF-data stored on it by enabling verification of their authenticity at the terminal-side. 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).

	Application Note 6: OT.Data_Authenticity from [PACEPP] shall be extended to all kinds of PACE terminals and EAC2 terminals.
OT.Data_Confidentiality	Confidentiality of Data The TOE must ensure confidentiality of the User Data and the TSF-data 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.
OT.Data_Integrity	Integrity of Data The TOE must ensure integrity of the User Data and the TSF-data stored on it by protecting these data against unauthorized modification (physical manipulation and unauthorized 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. Application Note 7: OT.Data_Integrity from [PACEPP] is extended here to all kinds of PACE terminals and EAC2 terminals. Justification: Obviously, data integrity must be ensured w.r.t. all possible terminal types.
OT.Identification	Identification of the TOE The TOE must provide means to store Initialization and Pre-Personalization Data in its non-volatile memory. The Initialization 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-Personalization data includes writing of the Personalization Agent Key(s).
OT.Prot_Abuse-Func	Protection against Abuse of Functionality 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, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.
OT.Prot_Inf_Leak	Protection against Information Leakage 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.
OT.Prot_Malfunction	Protection against Malfunctions 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.
OT.Prot_Phys-Tamper	Protection against Physical Tampering

	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.
OT.Tracing	Tracing travel document 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.

6.2. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

6.2.1. EAC2 Protection Profile

The following security objectives for the operational environment are listed in [PP-EAC2] and shall be considered for the present evaluation.

OE.Chip_Auth_Key	Key Pairs needed for Chip Authentication and Restricted Identification The electronic document issuer has to ensure that the electronic document's chip authentication key pair and the Restricted Identification key pair are generated securely, that the private keys of these key pairs are stored correctly in the electronic document's chip, and that the corresponding public keys are distributed to the EAC2 terminals that are used according to [TR03110-2] to check the authenticity of the electronic document's chip. Justification: The TSF of [PACEPP] does not include any mechanism to verify the authenticity of an electronic document (i.e. protection against cloning). Therefore, this additional security objective for the operational environment does not mitigate any threat of, and does not fulfill any OSP of [PACEPP].
OE.Terminal_Authentication	Key pairs needed for Terminal Authentication The electronic document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the electronic document issuer shall run a Country Verifying Certification Authority. The instances of the PKI shall fulfill the requirements and rules of the corresponding certificate policy. The electronic document issuer shall make the CVCA certificate available to the personalization agent or the manufacturer. Justification: The TSF of [PACEPP] does not include any mechanism to verify the authenticity of the terminal that reads out the data stored on the electronic document (by successfully executing PACE, a terminal only proves knowledge of

	the PACE password). Therefore, this additional security objective for the operational environment does not mitigate any threat of, and does not fulfill any OSP of [PACEPP].

6.2.2. PACE Protection Profile

According to [PP-EAC2], the following security objectives for the operational environment listed in [PACEPP] shall also be considered for the present evaluation.

OE.Legislative_Compliance	Issuing of the travel document The travel document Issuer must issue the travel document and approve it using the terminals complying with all applicable laws and regulations.
OE.Passive_Auth_Sign	Authentication of travel document by Signature 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 (CCSCA). 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 Personalization 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 organizations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.
OE.Personalisation	Personalisation of travel document The travel document Issuer must ensure that the Personalization Agents acting on his behalf (i) establish the correct identity of the travel document holder and create the biographical data for the travel document, (ii) enroll the biometric reference data of the travel document holder, (iii) write a subset of these data on the physical Passport (optical personalization) and store them in the travel document (electronic personalization) for the travel document holder as defined in [6], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [6] (in the role of a DS).
OE.Terminal	Terminal operating The terminal operators must operate their terminals as follows: 1.) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [6]. 2.) The related terminals implement the terminal parts of the PACE protocol [4], of the Passive Authentication [4] (by verification of the signature of the Document Security Object) and use them in this order. 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 CCSCA and CDS) 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, [6]). 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. Application Note 8: Opposite to OE.Terminal from [PACEPP], a terminal supporting EAC2 according to [TR03110-2] needs to store its own credentials for Extended Access Control and (if used) the Restricted Identity.
OE.Travel_Document_Holder	Travel document holder Obligations 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.

6.2.3. JCS Protection Profile

The following security objectives to the environment, derived from [PP-JCS], shall also be considered for the present evaluation, in order to address concerns related to post-issuance loading of applications.

OE.APPLET	No applet loaded post-issuance shall contain native methods.
OE.VERIFICATION	All the bytecodes shall be verified at least once before the loading, in order to ensure that each bytecode is valid at execution time. Additionally the applet shall follow all recommendations, if any, mandated in the platform guidance for maintaining the isolation property of the platform.
OE.CODE-EVIDENCE	For application code loaded during the Personalization phase (Phase 6), organizational measures or evaluated technical measures implemented by the TOE must ensure that the loaded application has not been changed since the code verifications required in OE.VERIFICATION. For application code loaded post-issuance and verified off-card according to the requirements of OE.VERIFICATION, the verification authority shall provide digital evidence to the TOE that the application code has not been modified after the code verification and that he is the actor who performed code verification.

6.3. SECURITY OBJECTIVES RATIONALE

6.3.1. Threats, OSPs and Assumptions coverage – Mapping table

	T.Counterfeit/EAC2	T.Sensitive_Data	T.Abuse-Func	T.Eavesdropping	T.Forgery	T.Information_Leakage	T.Malfunction	T.Phys-Tamper	T.Skimming	T.Tracing	P.EAC2_Terminal	P.RestrictedIdentity	P.Terminal_PKI	P.Card_PKI	P.Manufact	P.Pre-Operational	P.Terminal	P.Trustworthy_PKI	A.Passive_Auth	A.APPLET	A.VERIFICATION	A.CODE-EVIDENCE
OT.AC_Pers_EAC2					X											X						
OT.CA2	X																					
OT.Sens_Data_EAC2		X		X					X													
OT.Data_Authenticity					X				X													
OT.Data_Confidentiality				X					X													
OT.Data_Integrity					X				X													
OT.Identification															X	X						
OT.Prot_Abuse-Func			X		X																	
OT.Prot_Inf_Leak						X																
OT.Prot_Malfunction							X															
OT.Prot_Phys-Tamper					X			X														
OT.Tracing										X												
OE.Chip_Auth_Key	X										X											
OE.Terminal_Authentication		X							X		X		X									
OE.Legislative_Compliance																X						
OE.Passive_Auth_Sign					X									X				X	X			
OE.Personalisation					X											X						
OE.Terminal					X						X						X					
OE.Travel_Document_Holder										X												
OE.APPLET																				X		
OE.VERIFICATION																					X	
OE.CODE-EVIDENCE																						X

Table 2: Threats, OSP and assumptions coverage by security objectives – Mapping table

6.3.2. Coverage rationale

Note: Instead of copying verbatim text from [PACEPP], here only the rationale for new or altered threats and new or altered security objectives is given. The reader is invited to refer to [PACEPP] to get the rationale related to the remaining (unchanged) items.

The threat **T.Counterfeit/EAC2** addresses the attack of an unauthorized copy or reproduction of the genuine electronic document. This attack is countered by the proof of the chip's authenticity, as aimed by **OT.CA2** using a Chip Authentication key pair that is generated within the issuing PKI branch, as aimed by **OE.Chip_Auth_Key**. According to **OE.Chip_Auth_Key**, the terminal has to perform the Chip Authentication 2 protocol to verify the authenticity of the electronic document's chip.

The threat **T.Eavesdropping** addresses listening to the communication between the TOE and a PACE terminal or an EAC2 terminal in order to gain access to transferred user data. This threat is countered by the security objective **OT.Data_Confidentiality** through a trusted channel based on PACE Authentication, and by **OT.Sens_Data_EAC2** demanding a trusted channel that is based on Chip Authentication 2.

The threat **T.Forgery** addresses the fraudulent, complete or partial alteration of user data and/or TSF-Data stored on the TOE, and/or exchanged between the TOE and the terminal. In addition to the security objectives from [PACEPP] which counter this threat, the threat is also addressed by the refinement of OT.AC_Pers, here renamed **OT.AC_Pers_EAC2**.

The threat **T.Sensitive_Data** is countered by the TOE-Objective **OT.Sens_Data_EAC2**, that requires that read access to sensitive user data is only granted to EAC2 terminals with corresponding access rights. Furthermore, it is required that the confidentiality of the data is ensured during transmission. The objective **OE.Terminal_Authentication** requires the electronic document issuer to provide the public key infrastructure (PKI) to generate and distribute the card verifiable certificates needed by the electronic document to securely authenticate the EAC2 terminal.

The threat **T.Skimming** addresses accessing the user data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless/contact-based interface. Additionally to the security objectives from [PACEPP] which counter this threat, the threat is also addressed by **OT.Sens_Data_EAC2** that demands a trusted channel based on Chip Authentication 2, and requires that read access to sensitive user data is only granted to EAC2 terminals with corresponding access rights. Moreover, OE.Terminal_Authentication requires the electronic document issuer to provide the corresponding PKI.

The OSP **P.EAC2_Terminal** addresses the requirement for EAC2 terminals to implement the terminal parts of the protocols needed to executed EAC2 according to its specification in [TR03110-2], and to store (static keys) or generate (temporary keys and nonces) the needed related credentials. This is enforced by **OE.Chip_Auth_Key** which requires Chip Authentication and Restricted Identity keys to be correctly generated and stored, by **OE.Terminal_Authentication** for the PKI needed for Terminal Authentication, and by **OE.Terminal** which covers the PACE protocol and the Passive Authentication protocol.

P.Pre-Operational is enforced by security objectives from [PACEPP] that counter this OSP. In addition, the threat is also addressed by the refinement of OT.AC_Pers named **OT.AC_Pers_EAC2**.

The OSP **P.Terminal_PKI** is enforced by establishing the receiving PKI branch as aimed by the objective **OE.Terminal_Authentication**.

Additionally:

A.APPLET This assumption is upheld by the security objective for the operational environment OE.APPLET which ensures that no applet loaded post-issuance shall contain native methods.

A.VERIFICATION This assumption is upheld by the security objective on the operational environment OE.VERIFICATION which guarantees that all the bytecodes shall be verified at least once, before the loading, before the installation or before the execution in order to ensure that each bytecode is valid at execution time.

A.CODE-EVIDENCE This assumption is upheld by the security objective on the operational environment OE.CODE-EVIDENCE which ensures that evidences exist that the application code has been verified and not changed after verification.

6.4. COMPOSITION TASKS – OBJECTIVES PART

6.4.1. Statement of compatibility – TOE Objectives part

The following table (see next page) lists the relevant TOE security objectives of the MultiApp V4.0.1 platform, and provides the link to the composite-product TOE security objectives, showing that there is no contradiction between the two sets of objectives.

Label of the platform TOE security objective	Content of the platform TOE security objective	Linked Composite-product TOE security objectives
O.SID	The TOE shall uniquely identify every subject (applet, or package) before granting it access to any service.	OT.Sens_Data_EAC2 OT.Data_Confidentiality OT.Data_Integrity
O.FIREWALL	The TOE shall ensure controlled sharing of data containers owned by applets of different packages, or the JCRE and between applets and the TSFs.	OT.Sens_Data_EAC2 OT.Data_Confidentiality OT.Data_Integrity
O.GLOBAL_ARRAYS_CONFID	The TOE shall ensure that the APDU buffer that is shared by all applications is always cleaned upon applet selection. The TOE shall ensure that the global byte array used for the invocation of the install method of the selected applet is always cleaned after the return from the install method.	OT.Sens_Data_EAC2 OT.Data_Confidentiality
O.GLOBAL_ARRAYS_INTEG	The TOE shall ensure that only the currently selected applications may have a write access to the APDU buffer and the global byte array used for the invocation of the install method of the selected applet.	OT.CA2 OT.Data_Authenticity OT.Data_Integrity
O.NATIVE	The only means that the Java Card VM shall provide for an application to execute native code is the invocation of a method of the Java Card API, or any additional API.	OT.Sens_Data_EAC2 OT.Data_Confidentiality OT.Data_Integrity
O.OPERATE	The TOE must ensure continued correct operation of its security functions.	OT.Prot_Malfunction
O.REALLOCATION	The TOE shall ensure that the re-allocation of a memory block for the runtime areas of the Java Card VM does not disclose any information that was previously stored in that block.	OT.Sens_Data_EAC2 OT.Data_Confidentiality
O.RESOURCES	The TOE shall control the availability of resources for the applications.	OT.Prot_Malfunction
O.ALARM	The TOE shall provide appropriate feedback information upon detection of a potential security violation.	OT.Prot_Malfunction
O.CIPHER	The TOE shall provide a means to cipher sensitive data for applications in a secure way. In particular, the TOE must support cryptographic algorithms consistent with cryptographic usage policies and standards.	OT.Sens_Data_EAC2 OT.Data_Confidentiality
O.KEY-MNGT	The TOE shall provide a means to securely manage cryptographic keys. This concerns the correct generation, distribution, access and destruction of cryptographic keys.	OT.Sens_Data_EAC2 OT.Data_Confidentiality
O.PIN-MNGT	The TOE shall provide a means to securely manage PIN objects.	OT.Sens_Data_EAC2 OT.Data_Confidentiality OT.Data_Integrity
O.TRANSACTION	The TOE must provide a means to execute a set of operations atomically.	OT.Data_Integrity
O.OBJ-DELETION	The TOE shall ensure the object deletion shall not break references to objects.	OT.Data_Integrity
O.DELETION	The TOE shall ensure that both applet and package deletion perform as expected.	OT.Sens_Data_EAC2 OT.Data_Confidentiality
O.LOAD	The TOE shall ensure that the loading of a package into the card is safe. Besides, for codes loaded post-issuance, the TOE shall verify the integrity and authenticity evidences generated during the verification of the application package by the verification authority. This verification by the TOE shall occur during the load or late during the install process.	OT.Sens_Data_EAC2 OT.Data_Confidentiality OT.Data_Integrity
O.INSTALL	The TOE shall ensure that the installation of an applet performs as expected. Besides, for codes loaded post-issuance, the TOE shall verify the integrity and authenticity evidences generated during the verification of the application package by the verification authority. If not performed during the loading process, this verification by the TOE shall occur during the install process.	OT.Sens_Data_EAC2 OT.Data_Confidentiality OT.Data_Integrity

© Copyright Thales

Label of the platform TOE security objective	Content of the platform TOE security objective	Linked Composite-product TOE security objectives
O.SCP.RECOVERY	If there is a loss of power, or if the smart card is withdrawn from the CAD while an operation is in progress, the SCP must allow the TOE to eventually complete the interrupted operation successfully, or recover to a consistent and secure state.	OT.Prot_Malfunction
O.SCP.SUPPORT	The SCP shall support the TSFs of the TOE.	OT.Identification OT.Prot_Abuse-Func OT.Prot_Inf_Leak OT.Prot_Malfunction OT.Prot_Phys-Tamper
O.SCP.IC	The SCP shall provide all IC security features against physical attacks.	OT.Prot_Inf_Leak OT.Prot_Phys-Tamper
O.CARD-MANAGEMENT	The card manager shall control the access to card management functions such as the installation, update or deletion of applets. It shall also implement the card issuer's policy on the card. The card manager is an application with specific rights, which is responsible for the administration of the smart card. This component will in practice be tightly connected with the TOE, which in turn shall very likely rely on the card manager for the effective enforcing of some of its security functions. Typically the card manager shall be in charge of the life cycle of the whole card, as well as that of the installed applications (applets). The card manager should prevent that card content management (loading, installation, deletion) is carried out, for instance, at invalid states of the card or by non-authorized actors. It shall also enforce security policies established by the card issuer.	OT.Sens_Data_EAC2 OT.Data_Confidentiality OT.Data_Integrity OT.Prot_Abuse-Func
OT.AC_Pers	Access Control for Personalization of TOE and Applicative data: The TOE must ensure that the TOE and Application data requiring PACE usage and associated TSF data can be written by authorized Personalization Agents only in personalization phase. The TOE and Application data requiring PACE usage (e.g. logical travel document data in EF.DG1 to EF.DG16) and associated TSF data may be written only during and cannot be changed after personalization phase.	OT.AC_Pers_EAC2
OT.Data_Integrity	Integrity of Data: The TOE must ensure integrity of the User Data and the TSF-data stored on it by protecting these data against unauthorized modification (physical manipulation and unauthorized 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.	OT.Data_Integrity
OT.Data_Authenticity	Authenticity of Data: The TOE must ensure authenticity of the User Data and the TSF-data stored on it by enabling verification of their authenticity at the terminal-side. 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).	OT.Data_Authenticity
OT.Data_Confidentiality	Confidentiality of Data: The TOE must ensure confidentiality of the User Data and the TSF data 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.	OT.Data_Confidentiality
OT.Identification	Identification of the TOE: The TOE must provide means to store Initialization and Pre-Personalization Data in its non-volatile memory. The Initialization Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the application data requiring PACE usage (e.g. travel document for MRTD). The storage of the Pre-Personalization data includes writing of the Personalization Agent Key(s).	OT.Identification

© Copyright Thales

Label of the platform TOE security objective	Content of the platform TOE security objective	Linked Composite-product TOE security objectives
OT.Prot_Abuse_Func	Protection against Abuse of Functionality: 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, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.	OT.Prot_Abuse-Func
OT.Prot_Inf_Leak	Protection against Information Leakage: 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.	OT.Prot_Inf_Leak
OT.Prot_Phys_Tamper	Protection against Physical Tampering: 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.	OT.Prot_Phys-Tamper
OT.Prot_Malfunction	Protection against Malfunctions: 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.	OT.Prot_Malfunction
O.SpecificAPI	The TOE shall provide to application a specific API means to optimize control on sensitive operations performed by application. TOE shall provide services for secure array management and to detect loss of data integrity and inconsistent execution flow and react against tearing or fault induction.	OT.Sens_Data_EAC2 OT.Data_Confidentiality OT.Data_Integrity
O.RND	The TOE must contribute to ensure that random numbers shall not be predictable and shall have sufficient entropy.	OT.Sens_Data_EAC2 OT.Data_Confidentiality OT.Data_Integrity

6.4.2. Statement of compatibility – ENV Objectives part

The following table lists the relevant ENV security objectives related to the MultiApp V4.0.1 platform, and provides the link to the composite-product, showing that they have been taken into account and that no contradiction has been introduced.

Platform ENV security objective label	Platform ENV security objective content	Link to the composite-product
OE.VERIFICATION	All the bytecodes shall be verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. Additionally the applet shall follow all recommendations, if any, mandated in the platform guidance for maintaining the isolation property of the platform.	PPCA applet bytecodes have been verified and the applet follows the MultiApp V4.0.1 platform recommendations (covered by the present evaluation). For other applications which may be present on the composite-product: OE.VERIFICATION
OE.APPLET	No applet loaded post-issuance shall contain native methods.	The PPCA applet doesn't contain native methods. For other applications which may be present on the composite-product: OE.APPLET
OE.CODE-EVIDENCE	For application code loaded pre-issuance, evaluated technical measures implemented by the TOE or audited organizational measures must ensure that loaded application has not been changed since the code verifications required in OE.VERIFICATION. For application code loaded post-issuance and verified off-card according to the requirements of OE.VERIFICATION, the verification authority shall provide digital evidence to the TOE that the application code has not been modified after the code verification and that he is the actor who performed code verification.	Phases 1, 4 and 5: related processes are in the scope of the present evaluation and are audited through the ALC class. Phases 6 and 7: OE.CODE-EVIDENCE
OE.Prot_Logical_Data	Protection of TOE and applicative data: the inspection system of the applicative entity (e.g. receiving State or Organization) ensures the confidentiality and integrity of the data read from the TOE and applicative data (e.g. logical travel document). The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established.	OE.Terminal
OE.Personalisation	Personalization of TOE and application data requiring PACE usage: the Issuer must ensure that the Personalization Agents acting on his behalf establish the correct identity of the applicative user (e.g. travel document holder) and create the accurate applicative data and write them in TOE.	OE.Personalisation
OE.Terminal	Terminal operating: the terminal operators must operate their terminals as follows: 1.) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by application users (e.g.travel document presenter for MRTD) as defined in [PKI]. 2.) The related terminals implement the terminal parts of the PACE protocol [ICAO-TR-SAC]. 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 and their environment must ensure confidentiality and integrity of respective	OE.Terminal

	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 ST.	
OE.User_Obligations	The application user (e.g. 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.	OE.Travel_Document_Holder

7. Extended components definition

7.1. EXTENDED COMPONENTS FROM PACE-PP

7.1.1. Definition of the Family FAU_SAS

To describe the security functional requirements of the TOE, the family FAU_SAS of the class FAU (Security audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

The family 'Audit data storage (FAU_SAS)' is specified as follows:

Family behavior: This family defines functional requirements for the storage of audit data.

FAU_SAS.1 requires the TOE to provide the possibility to store audit data.

Management: There are no management activities foreseen.

Audit: There are no actions defined to be auditable.

FAU_SAS.1 Audit Storage

FAU_SAS.1.1 The TSF shall provide [assignment: authorized users] with the capability to store [assignment: list of audit information] in the audit records.

Hierarchical to: No other components
Dependencies: No dependencies.

7.1.2. Definition of the Family FCS_RND

To describe the IT security functional requirements of the TOE, the family FCS_RND of the class FCS (Cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND.1 is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

The family 'Generation of random numbers (FCS_RND)' is specified as follows:

Family behavior: This family defines quality requirements for the generation of random numbers intended to be used for cryptographic purposes.

FCS_RND.1 requires that random numbers meet a defined quality metric.

Management: There are no management activities foreseen.

Audit: There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric].

Hierarchical to: No other components
Dependencies: No dependencies.

7.1.3. Definition of the Family FMT_LIM

The family FMT_LIM describes the functional requirements for the test features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing abuse of functions by limiting the capabilities of the functions and by limiting their availability.

The family 'Limited capabilities and availability (FMT_LIM)' is specified as follows:

Family behavior: This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note, that FDP_ACF restricts access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

'FMT_LIM.1 Limited capabilities' requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

'FMT_LIM.2 Limited availability' requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.

Management: There are no management activities foreseen.

Audit: There are no actions defined to be auditable.

FMT_LIM.1 Limited capabilities

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 [assignment: Limited capability and availability policy].

Hierarchical to: No other components
Dependencies: FMT_LIM.2 Limited availability

FMT_LIM.2 Limited availability

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 [assignment: Limited capability and availability policy].

Hierarchical to: No other components
Dependencies: FMT_LIM.1 Limited capabilities

Application note: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume existence of two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the related policy. This also allows that

(i)the TSF is provided without restrictions in the product in its user environment, but its capabilities are so limited that the policy is enforced

or conversely

(ii)the TSF is designed with high functionality, but is removed or disabled in the product in its user environment.

The combination of both the requirements shall enforce the related policy.

7.1.4. Definition of the Family FPT_EMS

The family FPT_EMS (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations being not directly addressed by any other component of CC part 2.

The family 'TOE Emanation (FPT_EMS)' is specified as follows:

Family behavior: This family defines requirements to mitigate intelligible emanations.

'FPT_EMS.1 TOE emanation' has two constituents:

- 'FPT_EMS.1.1 Limit of Emissions' requires to not emit intelligible emissions enabling access to TSF data or user data.
- 'FPT_EMS.1.2 Interface Emanation' requires to not emit interface emanation enabling access to TSF data or user data.

Management: There are no management activities foreseen.

Audit: There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

FPT_EMS.1.2 The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

Hierarchical to: No other components
Dependencies: No dependencies

7.2. EXTENDED COMPONENTS FROM EAC2-PP

7.2.1. Definition of the Family FIA_API

To describe the IT security functional requirements of the TOE, the family FIA_API of the class FIA (Identification and authentication) is defined here. This family describes the functional requirements for proof of the claimed identity for the authentication verification by an external entity, where the other families of the class FIA address the verification of the identity of an external entity.

Application Note: Other families of the class FIA describe only the authentication verification of the user's identity performed by the TOE and do not describe the functionality of the TOE to prove its own

identity. The following paragraph defines the family FIA_API in the style of Common Criteria part 2 from a TOE point of view.

Family behavior: This family defines functions provided by the TOE to prove its identity and to be verified by an external entity in the TOE IT environment.

Management: The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or role, or of the TOE itself].

Hierarchical to: No other components
Dependencies: No dependencies

8. Security requirements

8.1. SECURITY FUNCTIONAL REQUIREMENTS

Note for SFR presentation:

- Selections and assignments already made in [PP-EAC2] are underlined.
- Selections and assignments made in the Security Target are written **in bold**, with a footnote mentioning the initial selection or assignment wording from [PP-EAC2].

8.1.1. Class FCS

FCS_CKM.1/DH_PACE(DH)
Cryptographic Key Generation – Diffie-Hellman for PACE and CA2 Session Keys

FCS_CKM.1.1/DH_PACE(DH) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Diffie-Hellman-Protocol compliant to [PKCS3]** [1] and specified cryptographic key sizes **listed in table 3** [2] that meet the following: [TR03110-2].

Key	Key size
SKPICC	1024, 1280, 1536 and 2048 bits
AESsession-DH	128, 192, and 256 bits

Table 3: Key sizes for FCS_CKM.1.1/DH_PACE(DH)

FCS_CKM.1/DH_PACE(ECDH)
Cryptographic Key Generation – Diffie-Hellman for PACE and CA2 Session Keys

FCS_CKM.1.1/DH_PACE(ECDH) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH compliant to [TR03111]]** [3] and specified cryptographic key sizes **listed in table 4** [4] that meet the following: [TR03110-2].

Key	Key size
SKPICC	160, 192, 224, 256, 320, 384, 512, and 521 bits
AESsession-ECDH	128, 192, 256

Table 4: Key sizes for FCS_CKM.1.1/DH_PACE(ECDH)

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

FCS_COP.1.1/SHA The TSF shall perform hashing in accordance with a specified cryptographic algorithm **SHA-1, SHA-224, SHA-256, SHA-384, SHA-512** [5] and cryptographic key sizes none that meet the following: [FIPS180-4]

[1] [selection: Diffie-Hellman-Protocol compliant to [PKCS3] , ECDH compliant to [TR03111]]
[2] [assignment: cryptographic key sizes]
[3] [selection: Diffie-Hellman-Protocol compliant to [PKCS3] , ECDH compliant to [TR03111]]
[4] [assignment: cryptographic key sizes]

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification

FCS_COP.1.1/SIG_VER The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm **listed in table 5** [6] and cryptographic key sizes **listed in table 5** [7] that meet the following: **standards listed in table 5** [8].

Iteration	Algorithm	Key size	Standards
(RSA_VER)	RSA (STD)	1024, 1280, 1536, 2048, 3072, and 4096	RSA SHA PKCS#1 RSA SHA PKCS#1 PSS
(ECC_VER)	ECC	160, 192, 224, 256, 320, 384, 512, 521	[TR-ECC] ECDSA SHA

Table 5: Signature verification algorithms, key lengths and standards

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

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

FCS_COP.1.1/PACE_ENC The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm AES in CBC mode and cryptographic key sizes **128, 192 and 256 bits** [9] that meet the following: [TR03110-3].

FCS_COP.1/PACE_MAC Cryptographic operation – CMAC

FCS_COP.1.1/PACE_MAC The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm CMAC and cryptographic key sizes **128, 192, 256 bits** [10] that meet the following: [TR03110-3].

FCS_CKM.4 Cryptographic key destruction – Session keys

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **secure erasing of the value** [11] that meets the following: **none**[12].

Application note: Secure erasing of data is performed by overwriting the data with either random numbers or 00h patterns.

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet **RGS [RGS-B1]**[13].

8.1.2. Class FIA

[5] [assignment: cryptographic algorithm]
[6] [assignment: cryptographic algorithm]
[7] [assignment: cryptographic key sizes]
[8] [assignment: list of standards]
[9] [selection: 128, 192, 256 bits]
[10] [selection: 128, 192, 256 bits]
[11] [assignment: cryptographic key destruction method]
[12] [assignment: list of standards]
[13] [assignment: a defined quality metric]

FIA_AFL.1/Suspend_PIN Authentication failure handling – Suspending PIN

FIA_AFL.1.1/Suspend_PIN The TSF shall detect when **an administrator configurable positive integer within [1 to 14] range** [14] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using the PIN as the shared password for PACE.

FIA_AFL.1.2/Suspend_PIN When the defined number of unsuccessful authentication attempts has been met, the TSF shall suspend the reference value of the PIN according to [TR03110-2].

FIA_AFL.1/Block_PIN Authentication failure handling – Blocking PIN

FIA_AFL.1.1/Block_PIN The TSF shall detect when **one** [15] unsuccessful authentication attempt occur related to consecutive failed authentication attempts using the suspended PIN as the shared password for PACE.

FIA_AFL.1.2/Block_PIN When the defined number of unsuccessful authentication attempts has been met, the TSF shall block the reference value of PIN according to [TR03110-2].

FIA_API.1/CA Authentication Proof of Identity

FIA_API.1.1/CA The TSF shall provide the protocol Chip Authentication 2 according to [TR03110-2], to prove the identity of the TOE.

FIA_UID.1/PACE Timing of identification

FIA_UID.1.1/PACE The TSF shall allow
1. To establish a communication channel,
2. Carrying out the PACE protocol according to [TR03110-2]
3. To read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS

on behalf of the user to be performed before the user is identified.
4. **None** [16]

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

FIA_UID.1/EAC2_Terminal Timing of identification

FIA_UID.1.1/EAC2_Terminal The TSF shall allow
1. To establish a communication channel,
2. Carrying out the PACE protocol according to [TR03110-2]
3. To read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
4. Carrying out the Terminal Authentication protocol 2 according to [TR03110-2]
5. **Performing PIN management activities through PACE secure channel** [17]

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

FIA_UID.1.2/EAC2_Terminal The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[14] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[15] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[16] [assignment: list of TSF-mediated actions]
[17] [assignment: list of TSF-mediated actions]

FIA_UAU.1/PACE	Timing of authentication

FIA_UAU.1.1/PACE The TSF shall allow
1. To establish a communication channel,
2. Carrying out the PACE protocol according to [TR03110-2]
3. To read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
4. **None** [18]

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

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

FIA_UAU.1/EAC2_Terminal	Timing of authentication

FIA_UAU.1.1/EAC2_Terminal The TSF shall allow
1. To establish a communication channel,
2. Carrying out the PACE protocol according to [TR03110-2],
3. To read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
4. Carrying out the Terminal Authentication 2 protocol according to [TR03110-2]

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

FIA_UAU.1.2/EAC2_Terminal The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Note: identification (FIA_UID.1/EAC2_Terminal) and authentication (FIA_UAU.1 /EAC2_Terminal) are performed simultaneously. Therefore, performing PIN management activities through PACE secure channel shall be allowed by the TSF before TA2 authentication.

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

FIA_UAU.4.1/PACE The TSF shall prevent reuse of authentication data related to
1. PACE protocol according to [TR03110-2],
2. Authentication Mechanism based on **AES** [19]
3. Terminal Authentication 2 protocol according to [TR03110-2]
4. **None** [20]

FIA_UAU.5/PACE	Multiple authentication mechanisms

FIA_UAU.5.1/PACE The TSF shall provide
1. PACE protocol according to [TR03110-2]
2. Passive Authentication according to [ICAO9303]
3. Secure messaging according to [TR03110-3]
4. Symmetric Authentication Mechanism based on **AES** [21]
5. Terminal Authentication 2 protocol according to [TR03110-2]
6. Chip Authentication 2 according to [TR03110-2]
7. **None** [22]

to support user authentication.

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

[18] [assignment: list of TSF-mediated actions]
[19] [selection: AES or other approved algorithms]
[20] [assignment: identified authentication mechanism(s)]
[21] [selection: AES or other approved algorithms]
[22] [assignment: list of multiple authentication mechanisms]

1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by the PACE protocol.
2. The TOE accepts the authentication attempt as personalization agent by **the SCP03 authentication mechanism** [23]
3. The TOE accepts the authentication attempt by means of the Terminal Authentication 2 protocol, only if (i) the terminal presents its static public key PKPCD and the key is successfully verifiable up to the CVCA and (ii) the terminal uses the PICC identifier IDPICC = Comp(ephem-PKPICC-PACE) calculated during, and the secure messaging established by the, current PACE authentication.
4. Having successfully run Chip Authentication 2, the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by Chip Authentication 2.
5. **None** [24]

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

FIA_UAU.6.1/CA The TSF shall re-authenticate the user under the conditions each command sent to the TOE after a successful run of Chip Authentication 2 shall be verified as being sent by the EAC2 terminal.

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

FIA_AFL.1.1/PACE The TSF shall detect when **the number listed in table 6** [25] unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password.

FIA_AFL.1.2/PACE When the defined number of unsuccessful authentication attempts has been met, the TSF shall take **the actions listed in table 6** [26].

Password type	Number	Action
MRZ, CAN	1	Exponentially increase time delay before new authentication attempt is possible.
PIN	An administrator configurable positive integer within [1 to 15] range	Block PIN
PUK	An administrator configurable positive integer within [1 to 15] range	Block PUK

Table 6: FIA_AFL.1/PACE Authentication failure handling

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

[23] [selection: the Authentication Mechanism with Personalization Agent Key(s)]
[24] [assignment: rules describing how the multiple authentication mechanisms provide authentication]
[25] [assignment: positive integer number]
[26] [assignment: list of actions]

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.

8.1.3. Class FDP

FDP_ACC.1/TRM	Subset access control – Terminal Access

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

1) Subjects:
- **a) Terminal,**
- **b) PACE terminal**
- **c) EAC2 terminal (Authentication Terminal)**

2) Objects:
- **a) All user data stored in the TOE; including sensitive user data**
- **b) All TOE intrinsic secret (i.e. cryptographic) data**

2) Operations: read, write and modify operations [27]

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

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

1) Subjects:
- a) Terminal,
- b) PACE terminal
- c) EAC2 terminal **(Authentication Terminal)** [28]

2) Objects:
- a) All user data stored in the TOE; including sensitive user data
- b) All TOE intrinsic secret (i.e. cryptographic) data

3) Security attributes:
- a) Terminal Authorization Level (access rights)

4) **None** [29].

FDP_ACF.1.2/TRM The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: a PACE terminal is allowed to read data objects from FDP_ACF.1/TRM after successful PACE authentication according to [TR03110-2], as required by FIA_UAU.1/PACE.

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

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

1. Any terminal not being a PACE terminal or an EAC2 terminal is not allowed to read, to write, to modify, or to use any user data stored on the electronic document
2. Terminals not using secure messaging are not allowed to read, write, modify, or use any data stored on the electronic document
3. No subject is allowed to read 'Communication Establishment Authorization Data' stored on the electronic document

[27] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[28] [assignment: list of EAC2 terminal types]
[29] [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]

4. No subject is allowed to write or modify 'secret electronic document holder authentication data' stored on the electronic document, except for PACE terminals or EAC2 terminals executing PIN management based on the following rules:
   - **After PACE authentication with PIN or PUK, the PIN value can be changed**
   - **Changing the PIN is only allowed to EAC2 terminals using the following mechanism: The TOE applies the EAC2 protocol (cf. FIA_UAU.5) to determine access rights of the terminal according to [TR03110-2]. To determine the effective authorization of a terminal, the chip must calculate a bitwise Boolean 'and' of the relative authorization contained in the CHAT of the Terminal Certificate, the referenced DV Certificate, and the referenced CVCA Certificate, and additionally the confined authorization sent as part of PACE. Based on that effective authorization and the terminal type drawn from the CHAT of the Terminal Certificate, the TOE shall grant the right to change the PIN**. [30]
5. No subject is allowed to read, write, modify, or use the private Restricted Identification key(s) and Chip Authentication key(s) stored on the electronic document.
6. Reading, modifying, writing, or using sensitive user data is only allowed to EAC2 terminals using the following mechanism: The TOE applies the EAC2 protocol (cf. FIA_UAU.5) to determine access rights of the terminal according to [TR03110-2]. To determine the effective authorization of a terminal, the chip must calculate a bitwise Boolean 'and' of the relative authorization contained in the CHAT of the Terminal Certificate, the referenced DV Certificate, and the referenced CVCA Certificate, and additionally the confined authorization sent as part of PACE. Based on that effective authorization and the terminal type drawn from the CHAT of the Terminal Certificate, the TOE shall grant the right to read, modify or write sensitive user data, or perform operations using these sensitive user data.
7. No subject is allowed to read, write, modify, or use the data objects 2b) of FDP_ACF.1.1/TRM.
8. **None**. [31]

FDP_RIP.1	Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects:
1. Session keys (PACE-KMAC, PACE-KEnc), (CA-KMAC, CA-KEnc) (immediately after closing related communication session)
2. The ephemeral private key ephem-SKPICC-PACE (by having generated a DH shared secret K)
3. Secret electronic document holder authentication data, e.g. PIN and/or PUK (when their temporarily stored values are not used any more)
4. **None**. [32]

FDP_UCT.1/TRM	Basic data exchange confidentiality – MRTD

FDP_UCT.1.1/TRM The TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorized disclosure.

FDP_UIT.1/TRM	Data exchange integrity

FDP_UIT.1.1/TRM The TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.

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

8.1.4. Class FTP

[30] [assignment: list of rules for PIN management chosen from [TR03110-2]]
[31] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[32] [assignment: list of objects]

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

FTP_ITC.1.1/PACE The TSF shall provide a communication channel between itself and a PACE terminal that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. The trusted channel shall be established by performing the PACE protocol according to [TR03110-2].

FTP_ITC.1.2/PACE The TSF shall permit a PACE terminal to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE The TSF shall enforce communication via the trusted channel for any data exchange between the TOE and a PACE terminal after PACE.

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

FTP_ITC.1.1/CA2 The TSF shall provide a communication channel between itself and an EAC2 terminal that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. The trusted channel shall be established by performing the CA2 protocol according to [TR03110-2].

FTP_ITC.1.2/CA2 The TSF shall permit an EAC2 terminal to initiate communication via the trusted channel.

FTP_ITC.1.3/CA2 The TSF shall enforce communication via the trusted channel for any data exchange between the TOE and an EAC2 terminal after Chip Authentication 2.

8.1.5. Class FAU

FAU_SAS.1	Audit storage

FAU_SAS.1.1 The TSF shall provide the Manufacturer with the capability to store the Initialization and Pre-Personalization Data in the audit records.

8.1.6. Class FMT

FMT_SMF.1	Specification of Management Functions

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. Resume and unblock the PIN (if any),
6. Activate and deactivate the PIN (if any).

FMT_SMR.1/PACE	Security roles

FMT_SMR.1.1/PACE The TSF shall maintain the roles
1. Manufacturer
2. Personalization Agent
3. Terminal
4. PACE terminal
5. Country Verifying Certification Authority

6. Document Verifier
7. EAC2 terminal **(Authentication Terminal)** [33]
8. Electronic document holder
9. **None**. [34]

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

Application Note: The role terminal is the default role for any terminal being recognized by the TOE as neither PACE terminal nor EAC2 terminal. The roles CVCA, DV, and EAC2 terminal are recognized by analyzing the current Terminal Certificate, cf. [TR03110-2], (FIA_UAU.1/EAC2_Terminal). Specific types of EAC2 terminals are identified analogously. The TOE recognizes the electronic document holder by using a PACE terminal together with inputs PIN or PUK (FIA_UAU.1/PACE).

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

FMT_MTD.1.1/CVCA_INI The TSF shall restrict the ability to write the
1. Initial CVCA Public Key,
2. Meta-data of the initial CVCA Certificate as required in [TR03110-2], resp. [TR03110-3],
3. Initial Current Date,
4. **None** [35]

to **the manufacturer and the personalization agent**. [36]

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

FMT_MTD.1.1/CVCA_UPD The TSF shall restrict the ability to update the
1. CVCA Public Key (PKCVCA),
2. Meta-data of the CVCA Certificate as required by [TR03110-2], resp. [TR03110-3],
3. **None** [37]

to the Country Verifying Certification Authority.

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

FMT_MTD.1.1/DATE The TSF shall restrict the ability to modify the current date to
1. CVCA
2. Document Verifier
3. EAC2 terminal **(Authentication Terminal)** [38] possessing an Accurate Terminal Certificate according to [TR03110-3]
4. **Domestic EAC1 terminal (Inspection System)** [39]

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

FMT_MTD.1.1/PA The TSF shall restrict the ability to write the card/chip security object(s) (SOC) and the document Security Object (SOD) to the Personalization Agent.

[33] [assignment: list of EAC2 terminal types]
[34] [assignment: the authorized identified roles]
[35] [assignment: list of TSF data]
[36] [selection: the manufacturer, the personalization agent]
[37] [assignment: list of TSF data]
[38] [assignment: list of EAC2 terminal types]
[39] [assignment: the authorized identified roles]

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

FMT_MTD.1.1/SK_PICC The TSF shall restrict the ability to **create and load** [40] the Chip Authentication private key(s) (SKPICC) and the Restricted Identification Private Key(s) to the personalization agent.

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

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to read the
1. PACE passwords,
2. Personalization Agent Keys,
3. Chip Authentication private key(s) (SKPICC)
4. Restricted Identification private key(s)
5. **None** [41]

to none.

FMT_MTD.1/Initialize_PIN **Management of TSF data – Initialize PIN**

FMT_MTD.1.1/Initialize_PIN The TSF shall restrict the ability to write the initial PIN and PUK to the personalization agent.

FMT_MTD.1/Resume_PIN **Management of TSF data – Resuming PIN**

FMT_MTD.1.1/Resume_PIN The TSF shall restrict the ability to resume the suspended PIN to the electronic document holder.

FMT_MTD.1/Change_PIN **Management of TSF data – Changing PIN**

FMT_MTD.1.1/Change_PIN The TSF shall restrict the ability to change the blocked PIN to:
- **The electronic document holder (using the PUK for changing the PIN)**
- **An EAC2 terminal of a type that has the terminal authorization level for PIN management.** [42]

FMT_MTD.1/Unblock_PIN **Management of TSF data – Unblocking PIN**

FMT_MTD.1.1/Unblock_PIN The TSF shall restrict the ability to unblock the blocked PIN to
1. The electronic document holder (using the PUK for unblocking),
2. An EAC2 terminal of a type that has the terminal authorization level for PIN management.

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

FMT_MTD.1.1/Activate_PIN The TSF shall restrict the ability to activate and deactivate the PIN to an EAC2 terminal of a type that has the terminal authorization level for PIN management.

FMT_MTD.3 Secure TSF data

[40] [selection: create, load]
[41] [assignment: list of TSF data]
[42] [assignment: the authorized identified roles that match the list of PIN changing rules conformant to [TR03110-2]]

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 2 and the Access Control SFP.

Refinement: To determine if the certificate chain is valid, the TOE shall proceed the certificate validation according to [TR03110-3].

FMT_LIM.1 Limited capabilities

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced: Deploying test features after TOE delivery do not allow

1. User Data to be manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. Software to be reconstructed,
4. Substantial information about construction of TSF to be gathered which may enable other attacks, and
5. **None** [43]

Application note: no test features are deployed after TOE delivery, meaning that this SFR is automatically enforced.

FMT_LIM.2 Limited availability

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced: Deploying test features after TOE delivery do not allow

1. User Data to be manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. Software to be reconstructed,
4. Substantial information about construction of TSF to be gathered which may enable other attacks, and
5. **None** [44]

Application note: no test features are available after TOE delivery, meaning that this SFR is automatically enforced.

FMT_MTD.1/INI_ENA
Management of TSF data – Writing Initialization and Pre-personalization Data

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

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

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to read out the Initialization Data and the Pre-personalization Data to the Personalization Agent.

[43] [assignment: Limited capability and availability policy]
[44] [assignment: Limited capability and availability policy]

8.1.7. Class FPT

FPT_EMS.1	TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **electromagnetic and current emissions** [45] in excess of **intelligible threshold** [46] enabling access to
1. The session keys (PACE-KMAC, PACE-KEnc), (CA-KMAC, CA-KEnc)
2. The ephemeral private key ephem-SKPICC-PACE
3. The Chip Authentication private keys (SKPICC)
4. The PIN, PUK
5. **None** [47]

And
6. The Restricted Identification private key(s) SKID
7. **None** [48].

FPT_EMS.1.2 The TSF shall ensure any users are unable to use the following interface electronic document's contactless/contact-based interface and circuit contacts to gain access to
1. The session keys (PACE-KMAC, PACE-KEnc), (CA-KMAC, CA-KEnc)
2. The ephemeral private key ephem - SKPICC- PACE1
3. The Chip Authentication private key(s) (SKPICC)
4. The PIN, PUK
5. **None** [49]

And
6. The Restricted Identification private key(s) SKID
7. **None**. [50]

FPT_FLS.1	Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:
1. Exposure to operating conditions causing a TOE malfunction,
2. Failure detected by TSF according to FPT_TST.1
3. **None**. [51]

FPT_TST.1	TSF testing

FPT_TST.1.1 The TSF shall run a suite of self-tests **at the conditions listed in table 7** [52] to demonstrate the correct operation of the TSF.

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

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

Conditions under which self-test should occur	Description of the self-test

[45] [assignment: types of emissions]
[46] [assignment: specified limits]
[47] [assignment: list of types of TSF data]
[48] [assignment: list of types of user data]
[49] [assignment: list of types of TSF data]
[50] [assignment: list of types of user data]
[51] [assignment: list of types of failures in the TSF]
[52] [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]]

During initial start-up	RNG live test, sensor test, FA detection, Integrity Check of NVM ES
Periodically	RNG monitoring, FA detection
After cryptographic computation	FA detection
Before any use or update of TSF data	FA detection, Integrity Check of related TSF data

Table 7: Self-tests

FPT_PHP.3	Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced.

8.2. SECURITY ASSURANCE REQUIREMENTS

This ST is based on the EAL4 assurance package augmented with the components ATE_DPT.2, AVA_VAN.5 and ALC_DVS.2.

8.3. SECURITY REQUIREMENTS RATIONALE

8.3.1. TOE security objectives coverage – Mapping table

	OT.Identifcation	OT.AC_Pers_EAC2	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confdentiality	OT.Tracing	OT.Prot_Abuse_Func	OT.Prot_Inf_Leak	OT.Prot_Phys_Tamper	OT.Prot_Malfunction	OT.CA2	OT.Sens_Data_EAC2
FCS_CKM.1/DH_PACE(DH)			X	X	X						X	X
FCS_CKM.1/DH_PACE(ECDH)			X	X	X						X	X
FCS_COP.1/SHA			X	X	X						X	X
FCS_COP.1/SIG_VER			X	X	X							X
FCS_COP.1/PACE_ENC					X							X
FCS_COP.1/PACE_MAC			X	X							X	
FCS_CKM.4			X	X	X							X
FCS_RND.1			X	X	X						X	X
FIA_AFL.1/Suspend_PIN		X	X	X	X							X
FIA_AFL.1/Block_PIN		X	X	X	X	X						X
FIA_API.1/CA			X	X	X						X	X
FIA_API.1/RI												
FIA_UID.1/PACE			X	X	X							X
FIA_UID.1/EAC2_Terminal		X	X	X	X							X
FIA_UAU.1/PACE			X	X	X							X
FIA_UAU.1/EAC2_Terminal		X	X	X	X							X

FIA_UAU.4/PACE			X	X	X						X
FIA_UAU.5/PACE			X	X	X						X
FIA_UAU.6/CA			X	X	X						X
FIA_AFL.1/PACE						X					
FIA_UAU.6/PACE			X	X	X						X
FDP_ACF.1/TRM		X	X		X						X
FDP_RIP.1		X	X	X	X					X	X
FDP_ACC.1/TRM		X	X		X						X
FDP_UCT.1/TRM			X		X						X
FDP_UIT.1/TRM			X		X						X
FTP_ITC.1/PACE			X	X	X	X					X
FTP_ITC.1/CA2			X	X	X	X					X
FAU_SAS.1	X	X									
FMT_SMF.1	X	X	X	X	X						X
FMT_SMR.1/PACE	X	X	X	X	X						X
FMT_MTD.1/CVCA_INI			X	X	X						X
FMT_MTD.1/CVCA_UPD			X	X	X						X
FMT_MTD.1/DATE			X	X	X						X
FMT_MTD.1/PA		X	X	X	X					X	X
FMT_MTD.1/SK_PICC			X	X	X					X	X
FMT_MTD.1/KEY_READ		X	X	X	X					X	X
FMT_MTD.1/Initialize_PIN		X	X	X	X						X
FMT_MTD.1/Resume_PIN		X	X	X	X						X
FMT_MTD.1/Change_PIN		X	X	X	X						X
FMT_MTD.1/Unblock_PIN		X	X	X	X						X
FMT_MTD.1/Activate_PIN		X	X	X	X						X
FMT_MTD.3			X	X	X						X
FMT_LIM.1							X				
FMT_LIM.2							X				
FMT_MTD.1/INI_ENA	X	X									
FMT_MTD.1/INI_DIS	X	X									
FPT_EMS.1								X			
FPT_FLS.1								X		X	
FPT_TST.1								X		X	
FPT_PHP.3			X					X	X		

Table 8: TOE Security Objectives coverage by SFRs – Mapping table

8.3.2. TOE security objectives coverage – Rationale

OT.Identification

The security objective OT.Identification addresses the storage of initialization and pre-personalization data in its non-volatile memory. This data includes the IC identification data that uniquely identify the TOE's chip. This is ensured by 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 related functions and roles.

OT.AC_Pers_EAC2

The security objective OT.AC_Pers_EAC2 ensures that only the personalization agent can write user- and TSF-Data into the TOE, and that some of this data cannot be altered after personalization. This property is covered by FDP_ACC.1/TRM and FDP_ACF.1/TRM requiring, amongst other, an appropriate authorization level of an EAC2 terminal. This authorization level can be achieved by terminal identification/authentication as required by the SFRs FIA_UID.1/EAC2_Terminal and FIA_UAU.1/EAC2_Terminal. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the related functions and roles. Since only an EAC2 terminal can reach the necessary authorization level, using and managing the PIN (the related SFRs are FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, and FMT_MTD.1/Activate_PIN, FMT_MTD.1/Initialize_PIN) also support the achievement of this objective. FDP_RIP.1 requires erasing the temporal values PIN and PUK. 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. FMT_MTD.1/PA covers the related property of OT.AC_Pers_EAC2 (writing/updating SOC and SOD and, in generally, personalization data). Updating such data can only be done by the personalization agent prior to the operational phase. Thus such data cannot be changed after the personalization of the document, as required by OT.AC_Pers_EAC2. Finally, FMT_MTD.1/KEY_READ ensures that cryptographic keys for EAC2 cannot be read by users.

OT.Data_Integrity

The security objective OT.Data_Integrity ensures that the TOE always ensures integrity of stored user- and TSF-Data and, after Terminal- and Chip Authentication 2, of these data exchanged (physical manipulation and unauthorized modifying). Physical manipulation is addressed by FPT_PHP.3.Unauthorized modifying of the stored data is addressed by FDP_ACC.1/TRM and FDP_ACF.1/TRM. Enforcement of the two previous in a protected manner is ensured by FDP_UCT.1/TRM and FDP_UIT.1/TRM. A specific authorization level is achieved by terminal identification/ authentication as required by the SFRs FIA_UID.1/EAC2_Terminal, FIA_UAU.1/EAC2_Terminal, supported by FCS_COP.1/SIG_VER. The TA2 protocol uses the result of PACE authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) being, in turn, supported by FCS_CKM.1/DH_PACE. Since PACE can use the PIN as the shared secret, using and management of PIN (FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Activate_PIN, FMT_MTD.1/Initialize_PIN) also support achievement of this objective. FDP_RIP.1 requires erasing the temporal values of PIN, PUK. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the used protocols. To allow for a verification of the certificate chain as required 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 required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. Unauthorized modifying of the exchanged data is addressed by FTP_ITC.1/CA2 and FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. FIA_API.1/CA using FCS_CKM.1/DH_PACE possessing the special properties FIA_UAU.5/PACE and FIA_UAU.6/CA. As a prerequisite of this trusted channel a trusted channel established with the PACE protocol using

FIA_UID.1/PACE, FIA_UAU.1/PACE and FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE.
CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT_MTD.1/SK_PICC governs creating/loading SKPICC, and FMT_MTD.1/KEY_READ requires SKPICC to be unreadable by users; thus its value remains confidential. FDP_RIP.1 requires erasing the values of SKPICC and session keys (here: for KMAC).FMT_MTD.1/PA requires that the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication is allowed to be modified only by the personalization agent. Hence, is to considered as trustworthy. The SFRs FCS_COP.1/SHA and FCS_RND.1 represent general support required for cryptographic operations. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support related functions and roles.

OT.Data_Authenticity
The security objective OT.Data_Authenticity ensures the authenticity of user- and TSF-Data (after Terminal- and the Chip Authentication 2) by enabling its verification on both the terminal-side and by an active verification by the TOE itself. This objective is mainly achieved by FTP_ITC.1/CA2 and FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. FIA_API.1/CA using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, and FIA_UAU.6/CA. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA_UID.1/PACE, FIA_UAU.1/PACE and FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE.
CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT_MTD.1/SK_PICC governs creating/loading SKPICC, FMT_MTD.1/KEY_READ requires to make this key unreadable by users. Hence its value remains confidential. FDP_RIP.1 requires to erase the values of SKPICC and session keys, here for KMAC.
FMT_MTD.1/PA requires that the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication is allowed to be modified only by the personalization agent only. Hence is to consider as trustworthy. A prerequisite for successful CA2 is an accomplished TA2 as required by FIA_UID.1/EAC2_Terminal, FIA_UAU.1/EAC2_Terminal, supported by FCS_COP.1/SIG_VER. The TA2 protocol uses the result of the PACE authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) being, in turn, supported by FCS_CKM.1/DH_PACE. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FMT_MTD.1/Resume_PIN, MT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Activate_PIN) also support achieving this objective. FDP_RIP.1 requires to erase the temporal values of the PIN and PUK.FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/CA and FCS_CKM.4 represent some specific required properties of the used protocols. To allow for a verification of the certificate chain as required in FMT_MTD.3, the CVCA's public key and certificate, as well as the current date, are written or updated by authorized identified roles as required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. The SFRs FCS_COP.1/SHA and FCS_RND.1 represent the general required support for cryptographic operations. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the related functions and roles.
OT.Data_Confidentiality
The security objective OT.Data_Confidentiality ensures that the TOE always ensures confidentiality of the user- and TSF-Data stored and, after Terminal- and Chip Authentication 2, of their exchange. This objective for the data stored is mainly achieved by FDP_ACC.1/TRM and FDP_ACF.1/TRM. Enforcement of the two previous in a protected manner is ensured by FDP_UCT.1/TRM and FDP_UIT.1/TRM. A specific authorization level is achieved by terminal identification/authentication as required by the SFRs FIA_UID.1/EAC2_Terminal, FIA_UAU.1/EAC2_Terminal, supported by FCS_COP.1/SIG_VER. The TA2 protocol uses the result of the PACE authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE, confidentiality of the PACE passwords is ensured by FMT_MTD.1/KEY_READ) being, in turn, supported by FCS_CKM.1/DH_PACE. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA_AFL.1/Suspend_PIN,

FIA_AFL.1/Block_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Change_PIN, MT_MTD.1/Initialize_PIN, FMT_MTD.1/Activate_PIN) also support to achieve this objective. FDP_RIP.1 requires erasing the temporal values of the PIN and PUK.FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE and FCS_CKM.4 represent some specific properties of the used protocols. To allow for a verification of the certificate chain as required in FMT_MTD.3, the CVCA's public key and certificate as well as the current date are written or updated by authorized identified role as required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. This objective for the data exchanged is mainly achieved by FTP_ITC.1/CA2 and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. FIA_API.1/CA using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, and FIA_UAU.6/CA. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA_UID.1/PACE, FIA_UAU.1/PACE and FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE.
CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT_MTD.1/SK_PICC governs creating/loading SKPICC, FMT_MTD.1/KEY_READ requires making this key unreadable by users. Thus its value remains confidential. FDP_RIP.1 requires erasing the values of SKPICC and session keys, here for KENC.FMT_MTD.1/PA requires that only the personalization agent is allowed to modify the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication. The SFRs FCS_COP.1/SHA and FCS_RND.1 represent the general required support for cryptographic operations. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the related functions and roles.

OT.Sens_Data_EAC2

The security objective of OT.Sens_Data_EAC2 aims to explicitly protect sensitive (as opposed to common) user and TSF-Data. This is mainly achieved by enforcing (FDP_UCT.1/TRM and FDP_UIT.1/TRM) the access control SFPs FDP_ACC.1/TRM and FDP_ACF.1/TRM.A specific authorization level is achieved by terminal identification/authentication as required by the SFRs FIA_UID.1/EAC2_Terminal, FIA_UAU.1/EAC2_Terminal, supported by FCS_COP.1/SIG_VER. The TA2 protocol uses the result of the PACE authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE, confidentiality of the PACE passwords is ensured by FMT_MTD.1/KEY_READ) being, in turn, supported by FCS_CKM.1/DH_PACE. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FMT_MTD.1/Resume_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN, FMT_MTD.1/Activate_PIN) also support to achieve this objective. FDP_RIP.1 requires erasing the temporal values of the PIN and PUK.
FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE and FCS_CKM.4 represent some specific properties of the used protocols. To allow for a verification of the certificate chain as required in FMT_MTD.3, the CVCA's public key and certificate as well as the current date are written or updated by authorized identified role as required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. This objective for the data exchanged is mainly achieved by FTP_ITC.1/CA2 and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. FIA_API.1/CA using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, and FIA_UAU.6/CA. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA_UID.1/PACE, FIA_UAU.1/PACE and FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE.
CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT_MTD.1/SK_PICC governs creating/loading SKPICC, FMT_MTD.1/KEY_READ requires making this key unreadable by users. Thus its value remains confidential. FDP_RIP.1 requires erasing the values of SKPICC and session keys, here for KENC.FMT_MTD.1/PA requires that only the personalization agent is allowed to modify the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication. The SFRs FCS_COP.1/SHA and FCS_RND.1 represent

the general required support for cryptographic operations. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the related functions and roles.

OT.Prot_Abuse_Func
The rationale is analogous to [PACEPP].

OT.Prot_Phys_Tamper
The rationale is analogous to [PACEPP].

OT.Prot_Malfunction
The rationale is analogous to [PACEPP].

OT.Tracing
The security objective OT.Tracing ensures that the TOE prevents gathering TOE tracing data by means of unambiguously identifying the electronic document remotely through establishing or listening to communication via the contactless/contact-based interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ, PIN, PUK).This objective is achieved as follows:

1. While establishing PACE communication with CAN, MRZ or PUK (non-blocking authentication / authorization data) by FIA_AFL.1/PACE,
2. While establishing PACE communication using the PIN (blocking authentication data) by FIA_AFL.1/Block_PIN,
3. For listening to PACE communication and for establishing CA2 communication (which is of importance for the current PP, if Chip Security Object and PKPICC are card-individual) by FTP_ITC.1/PACE,
4. And for listening to CA2 communication (readable and writable user data: document details data, biographic data, biometric reference data) by FTP_ITC.1/CA2.

OT.CA2
The security objective OT.CA2 aims at enabling verification of the authenticity of the TOE as a whole device. This objective is mainly achieved by FIA_API.1/CA using FCS_CKM.1/DH_PACE. CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT_MTD.1/SK_PICC governs creating/loading SKPICC, whereas FMT_MTD.1/KEY_READ requires making this key unreadable by users. Hence, its value remains confidential. FDP_RIP.1 requires erasing the values of SKPICC and the session keys, here for CMAC. The authentication token TPICC is calculated using FCS_COP.1/PACE_MAC. The SFRs FCS_COP.1/SHA and FCS_RND.1 represent the general required support for cryptographic operations.FMT_MTD.1/PA requires that the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication is allowed to be modified only by the personalization agent only. Hence is to consider as trustworthy.

OT.Prot_Inf_Leak
The security objective OT.Prot_Inf_Leak aims at protection against disclosure of confidential user- or/and TSF-data stored on or processed by the TOE. This objective is achieved by

1. FPT_EMS.1 for 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,
2. FPT_FLS.1 and FPT_TST.1 for forcing a malfunction of the TOE, and
3. By FPT_PHP.3 for a physical manipulation of the TOE.

8.3.3. SFR dependency rationale

Security Functional Requirement	CC dependencies	Satisfied dependencies

Security Functional Requirement	CC dependencies	Satisfied dependencies
FCS_CKM.1/DH_PACE (DH)	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4 **See rationale**
FCS_CKM.1/DH_PACE (ECDH)	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4 **See rationale**
FCS_COP.1/SHA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	**See rationale**
FCS_COP.1/SIG_VER	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	**See rationale**
FCS_COP.1/PACE_ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/DH_PACE(DH) FCS_CKM.1/DH_PACE (ECDH) FCS_CKM.4
FCS_COP.1/PACE_MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/DH_PACE(DH) FCS_CKM.1/DH_PACE (ECDH) FCS_CKM.4
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/DH_PACE(DH) FCS_CKM.1/DH_PACE (ECDH)
FCS_RND.1	No dependencies	
FIA_AFL.1/Suspend_PIN	(FIA_UAU.1)	FIA_UAU.1/PACE
FIA_AFL.1/Block_PIN	(FIA_UAU.1)	FIA_UAU.1/PACE
FIA_API.1/CA	No dependencies	
FIA_UID.1/PACE	No dependencies	
FIA_UID.1/EAC2_Terminal	No dependencies	
FIA_UAU.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE
FIA_UAU.1/EAC2_Terminal	(FIA_UID.1)	FIA_UID.1/EAC2_Terminal
FIA_UAU.4/PACE	No dependencies	
FIA_UAU.5/PACE	No dependencies	
FIA_UAU.6/CA	No dependencies	
FIA_AFL.1/PACE	(FIA_UAU.1)	FIA_UAU.1/PACE
FIA_UAU.6/PACE	No dependencies	
FDP_ACF.1/TRM	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/TRM **See rationale**
FDP_RIP.1	No dependencies	
FDP_ACC.1/TRM	(FDP_ACF.1)	FDP_ACF.1/TRM
FDP_UCT.1/TRM	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FTP_ITC.1/PACE FDP_ACC.1/TRM
FDP_UIT.1/TRM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FTP_ITC.1/PACE FDP_ACC.1/TRM
FTP_ITC.1/PACE	No dependencies	
FTP_ITC.1/CA2	No dependencies	
FAU_SAS.1	No dependencies	
FMT_SMF.1	No dependencies	
FMT_SMR.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE FIA_UID.1/EAC2_Terminal
FMT_MTD.1/CVCA_INI	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/DATE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.1/PACE

© Copyright Thales

Security Functional Requirement	CC dependencies	Satisfied dependencies
FMT_MTD.1/PA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/SK_PICC	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/Initialize_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/Resume_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/Change_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/Unblock_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/Activate_PIN	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.3	(FMT_MTD.1)	MT_MTD.1/CVCA_INI FMT_MTD.1/CVCA_UPD FMT_MTD.1/DATE
FMT_LIM.1	(FMT_LIM.2)	FMT_LIM.2
FMT_LIM.2	(FMT_LIM.1)	FMT_LIM.1
FMT_MTD.1/INI_ENA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/INI_DIS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1 FMT_SMR.1/PACE
FPT_EMS.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_TST.1	No dependencies	
FPT_PHP.3	No dependencies	

Rationale for the exclusion of dependencies:

- The dependencies (FCS_CKM.2 or FCS_COP.1) of FCS_CKM.1/DH_PACE(DH) and FCS_CKM.1/DH_PACE (ECDH) are unsupported. Indeed, a Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.
- The dependencies of FCS_COP.1/SHA are unsupported. Indeed, a hash function does not use any cryptographic key, therefore no key import, no key generation and no key destruction can be expected here.
- The dependencies of (FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) of FCS_COP.1/SIG_VER are unsupported:
  - The root key PKCVCA (initialization data) used for verifying the DV Certificate is stored in the TOE during its personalization in the card issuing life cycle phase. Since importing the respective certificates (Terminal Certificate, DV Certificate) does not require any special security measures except those required by the current SFR (cf. FMT_MTD.3), the Protection Profile does not contain any dedicated requirement like FDP_ITC.2 for the import function.
  - Cryptographic keys used for the purpose of the current SFR (PKPCD, PKDV, PKCVCA) are public keys; they do not represent any secret, and hence need not to be destroyed

- The dependency (FMT_MSA.3) of FDP_ACF.1/TRM is unsupported. Indeed, the access control TSF according to FDP_ACF.1/TRM uses security attributes that have been defined during personalization, and that are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

8.3.4. SAR – Evaluation Assurance Level Rationale

The EAL4 package and addition of ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 are required by [PP-EAC2].

8.3.5. SAR – Dependency rationale

Security Assurance Requirement	CC dependencies	Satisfied dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4 ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3 ALC_TAT.1
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4 ALC_DVS.2 ALC_LCD.1
ALC_CMS.4	No dependencies	
ALC_DEL.1	No dependencies	
ALC_DVS.2	No dependencies	
ALC_LCD.1	No dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1 ASE_INT.1 ASE_REQ.2
ASE_ECD.1	No dependencies	
ASE_INT.1	No dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1 ASE_OBJ.2
ASE_SPD.1	No dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4 ASE_INT.1 ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4 ATE_FUN.1
ATE_DPT.2	(ADV_ARC.1) and (ADV_TDS.3) and (ATE_FUN.1)	ADV_ARC.1 ADV_TDS.3 ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4 AGD_OPE.1 AGD_PRE.1 ATE_COV.2 ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1 ADV_FSP.4 ADV_IMP.1 ADV_TDS.3 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1

The table here-above shows that all SAR dependencies are met.

8.4. COMPOSITION TASKS – SFR PART

The following table (see next page) lists the SFRs that are declared in the security target [ST_PLT], and separates them in relevant platform[53]-SFRs (RP_SFR) and irrelevant platform-SFRs (IP_SFR), as requested in [CCDB]. No contradictions have been found between the RP_SFR set and the SFRs related to the composite-product.

[53] Using the composition tasks terminology, the platform is the MultiApp V4.0.1 javacard platform.

Platform SFR	RP_SFR	IP_SFR	Compatibility with composite-product SFRs
FDP_IFC.1/JCVM	X		No contradiction
FDP_IFF.1/JCVM	X		No contradiction
FDP_RIP.1/OBJECTS	X		No contradiction
FMT_MSA.2/FIREWALL_JCVM	X		No contradiction
FMT_MSA.3/FIREWALL	X		No contradiction
FMT_MSA.3/JCVM	X		No contradiction
FMT_SMR.1/JCRE	X		No contradiction
FMT_SMF.1/CORE_LC	X		No contradiction
FCS_CKM.1	X		No contradiction
FCS_CKM.2	X		No contradiction
FCS_CKM.3	X		No contradiction
FCS_CKM.4	X		No contradiction
FCS_COP.1	X		No contradiction
FDP_RIP.1/APDU	X		No contradiction
FDP_RIP.1/bArray	X		No contradiction
FDP_RIP.1/ABORT	X		No contradiction
FDP_RIP.1/KEYS	X		No contradiction
FDP_ROL.1/FIREWALL	X		No contradiction
FAU_ARP.1	X		No contradiction
FDP_SDI.2	X		No contradiction
FPT_TDC.1	X		No contradiction
FPT_FLS.1/JCS	X		No contradiction
FPR_UNO.1	X		No contradiction
FMT_MTD.1/JCRE	X		No contradiction
FMT_MTD.3/JCRE	X		No contradiction
FIA_ATD.1/AID	X		No contradiction
FIA_UID.2/AID	X		No contradiction
FIA_USB.1/AID	X		No contradiction
FDP_ITC.2/Installer	X		No contradiction
FMT_SMR.1/Installer	X		No contradiction
FPT_FLS.1/Installer	X		No contradiction
FPT_RCV.3/Installer	X		No contradiction
FMT_MSA.1/ADEL	X		No contradiction
FMT_MSA.3/ADEL	X		No contradiction
FMT_SMR.1/ADEL	X		No contradiction
FMT_SMF.1/ADEL	X		No contradiction
FDP_ACC.2/ADEL	X		No contradiction
FDP_ACF.1/ADEL	X		No contradiction
FDP_RIP.1/ADEL	X		No contradiction
FPT_FLS.1/ADEL	X		No contradiction
FDP_ACC.2/FIREWALL	X		No contradiction
FDP_ACF.1/FIREWALL	X		No contradiction
FMT_MSA.1/JCRE	X		No contradiction
FMT_MSA.1/JCVM	X		No contradiction
FDP_RIP.1/TRANSIENT	X		No contradiction
FDP_RIP.1/ODEL	X		No contradiction
FPT_FLS.1/ODEL	X		No contradiction
FMT_MSA.1/CM	X		No contradiction
FMT_MSA.3/CM	X		No contradiction
FMT_SMR.1/CM	X		No contradiction
FMT_SMF.1/CM	X		No contradiction
FCO_NRO.2/CM	X		No contradiction
FIA_UAU.1/CM	X		No contradiction
FIA_UID.1/CM	X		No contradiction
FDP_IFC.2/CM	X		No contradiction
FDP_IFF.1/CM	X		No contradiction
FDP_UIT.1/CM	X		No contradiction

© Copyright Thales

Platform SFR	RP_SFR	IP_SFR	Compatibility with composite-product SFRs
FTP_ITC.1/CM	X		No contradiction
FPT_TST.1/SCP	X		No contradiction
FPT_PHP.3/SCP	X		No contradiction
FPT_RCV.4/SCP	X		No contradiction
FDP_ACC.1/CMGR	X		No contradiction
FDP_ACF.1/CMGR	X		No contradiction
FMT_MSA.1/CMGR	X		No contradiction
FMT_MSA.3/CMGR	X		No contradiction
FPT_FLS.1/SpecificAPI	X		No contradiction
FPT_ITT.1/SpecificAPI	X		No contradiction
FPR_UNO.1/SpecificAPI	X		No contradiction
FCS_RND.1	X		No contradiction
FCS_CKM.1/DH_PACE	X		No contradiction
FCS_CKM.1/PERSO	X		No contradiction
FCS_CKM.4/PACE	X		No contradiction
FCS_COP.1/PACE_ENC	X		No contradiction
FCS_COP.1/PACE_MAC	X		No contradiction
FCS_COP.1/PERSO	X		No contradiction
FCS_RND.1/PACE	X		No contradiction
FDP_RIP.1/PACE	X		No contradiction
FIA_AFL.1/PERSO	X		No contradiction
FIA_AFL.1/PACE	X		No contradiction
FIA_UID.1/PERSO	X		No contradiction
FIA_UAU.1/PERSO	X		No contradiction
FIA_UID.1/PACE	X		No contradiction
FIA_UAU.1/PACE	X		No contradiction
FIA_UAU.4/PACE	X		No contradiction
FIA_UAU.5/PACE	X		No contradiction
FIA_UAU.6/PACE	X		No contradiction
FTP_ITC.1/PACE	X		No contradiction
FMT_SMF.1/PACE	X		No contradiction
FMT_SMF.1/PERSO	X		No contradiction
FMT_SMR.1/PACE	X		No contradiction
FMT_SMR.1/PERSO	X		No contradiction
FMT_LIM.1/PERSO	X		No contradiction
FMT_LIM.2/PERSO	X		No contradiction
FMT_MTD.1/INI_ENA	X		No contradiction
FMT_MTD.1/INI_DIS	X		No contradiction
FMT_MTD.1/KEY_READ	X		No contradiction
FPT_EMS.1	X		No contradiction
FPT_FLS.1	X		No contradiction
FPT_TST.1	X		No contradiction
FPT_PHP.3	X		No contradiction

© Copyright Thales

9. TOE summary specification

9.1. THALES EMBEDDED SOFTWARE

The following TOE Security Functions are provided by the Thales Embedded Software:

SF.REL

- The TSF detects abnormal operating conditions. More generally, the TSF implements several categories of self-tests and take appropriate actions to always remain in a secure state.
- The TSF protects itself against information leakage. For that purpose, the TSF limits its current and electromagnetic emissions so as they remain non-exploitable by attackers with a high attack potential.

SF.CRYPTO

- The TSF generates AES session keys for PACE and CA2, based on either the Diffie-Hellman-Protocol compliant to [PKCS3] or ECDH compliant to [TR03111]]. In both cases the generation is done according to the [TR03110-2] specification.
- The TSF performs SHA1, SHA-224, SHA-256, SHA-384 and SHA-512 hashing according to [FIPS180-4]
- For the purpose of Terminal Authentication 2 according to [TR03110-2], the TSF implements digital signature verification based on RSA SHA PKCS#1 and ECDSA SHA.
- The TSF implements AES CBC and CMAC primitives with key lengths of 128, 192 or 256 bits
- Values of private keys and secret keys can never be read.
- The TSF securely erases private and secret keys when deallocated or no more needed.
- The TSF generates random numbers that meet the [RGS-B1] quality.

SF.SM

- The TSF performs secure messaging AES CBC encryption and decryption according to [TR03110-3]
- The TSF performs secure messaging CMAC generation and verification according to [TR03110-3]
- The secure messaging allows the TSF to transmit and receive user data in a manner protected from unauthorized disclosure.
- The secure messaging allows the TSF to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.
- The TSF implements secure messaging with PACE terminals according to [TR03110-2] and the PACE protocol.
- The TSF implements secure messaging with EAC2 terminals according to [TR03110-2] and the CA2 protocol

SF.MANUFACT_PERSO

- The TSF maintains the Manufacturer and Personalizer roles.
- The TSF supports initialization, Pre-personalization and Personalization operations.
- Initialization and pre-personalization operations are restricted the Manufacturer.
- The TSF provides the Manufacturer with the capability to store the Initialization and Pre-Personalization Data in the audit records.
- Only the Personalizer is able to read-out the Pre-personalization data loaded by the Manufacturer.
- Only the Personalizer is able to create and load the Chip Authentication private keys (SKPICC) and the Restricted Identification Private Keys.

- Only the Personalizer is able to write the card/chip security object(s) (SOC) and the document Security Object (SOD).
- Only the Manufacturer and Personalizer are able to write the Initial CVCA Public Key, the Initial Current Date and the Meta-data of the initial CVCA Certificate as required in [TR03110-2], resp. [TR03110-3].
- Only the Personalizer is able to write the initial PIN and PUK.
- The TSF implements the SCP03 secure channel for secure authentication of the Personalizer.

SF.PIN_PUK

- The TSF supports PIN resume and unblock operations
- The TSF supports PIN activate and deactivate operations
- The PIN can be changed after PACE authentication with PIN or PUK, or by an EAC2 Terminal having the corresponding authorization level.
- The TSF implements a PIN Try Limit (PTL) configured during Personalization. Once the limit is reached, the PIN is suspended. Only the electronic document holder is able to resume the suspended PIN. If a wrong PIN is presented one more time, the PIN is blocked.
- The blocked PIN can be changed only by:
  - The electronic document holder (using the PUK)
  - An EAC2 terminal of a type that has the terminal authorization level for PIN management
- The blocked PIN can be unblocked only by:
  - The electronic document holder (using the PUK)
  - An EAC2 terminal of a type that has the terminal authorization level for PIN management
- Only an EAC2 terminal of a type that has the terminal authorization level for PIN management is able to activate and deactivate the PIN.
- The TSF also implements a Try Limit for the PUK. This limit is configured during Personalization. Once the limit is reached, the PUK is blocked.
- PIN/PUK reference values can never be read.
- PIN/PUK temporarily stored values are securely erased as soon as PIN/PUK verification operations are completed.

SF.AC

The TSF enforces an access control policy based on the terminal and data to be accessed. The related attributes for Access Control enforcement are the Terminal Authorization Level (access rights). Read, write, modify and use operations are controlled. The TSF enforces the rules in FDP_ACF.1/TRM.

SF.AUTH

- The TSF provides the following authentication mechanisms to support user authentication:
  - Chip Authentication 2 protocol according to [TR03110-2]
  - Restricted Identification protocol according to [TR03110-2]
  - PACE protocol according to [TR03110-2]
  - Terminal Authentication 2 protocol according to [TR03110-2]
  - Passive Authentication according to [ICAO9303]
  - Secure messaging according to [TR03110-3]
  - Symmetric Authentication Mechanism based on AES
- The TSF allows a limited number of operations to be done before the user is identified/ authenticated through the PACE protocol. These allowed operations are listed in FIA_UID.1/PACE / FIA_UAU.1/PACE respectively.
- The TSF allows a limited number of operations to be done before the user is identified/ authenticated through the EAC2 protocol. These allowed operations are listed in FIA_UID.1/EAC2_Terminal / FIA_UAU.1/EAC2_Terminal respectively.

© Copyright Thales

- The TSF prevents the reuse of authentication data related to:
  - PACE protocol according to [TR03110-2]
  - Authentication Mechanism based on AES
  - Terminal Authentication 2 protocol according to [TR03110-2]
- The TSF authenticates any user's claimed identity according to the following rules:
  - Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by the PACE protocol.
  - The TOE accepts the authentication attempt as personalization agent by the SCP03 authentication mechanism
  - The TOE accepts the authentication attempt by means of the Terminal Authentication 2 protocol, only if (i) the terminal presents its static public key PKPCD and the key is successfully verifiable up to the CVCA and (ii) the terminal uses the PICC identifier IDPICC = Comp(ephem-PKPICC-PACE) calculated during, and the secure messaging established by the, current PACE authentication.
  - Having successfully run Chip Authentication 2, the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by Chip Authentication 2.
- Re-authentication:
  - The TSF re-authenticates the user under the conditions each command sent to the TOE after a successful run of Chip Authentication 2 shall be verified as being sent by the EAC2 terminal
  - The TSF re-authenticates 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

SF.MNGT

- The TSF maintains the roles: Manufacturer, Personalization Agent, Terminal, PACE terminal, Country Verifying Certification Authority, Document Verifier, EAC2 terminal (Authentication Terminal) and Electronic document holder.
- Only the Country Verifying Certification Authority is able to update the CVCA Public Key (PKCVCA) and the Meta-data of the CVCA Certificate as required by [TR03110-2], resp. [TR03110-3]
- Only the CVCA, Document Verifier, Domestic EAC1 terminal (Inspection System) and EAC2 terminal (Authentication Terminal) possessing an Accurate Terminal Certificate according to [TR03110-3] are able to modify the current date.
- The TSF ensures that only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication protocol 2 and the Access Control policy. To determine if the certificate chain is valid, the TOE proceeds the certificate validation according to [TR03110-3].

9.2. M7892 INTEGRATED CIRCUIT

The following M7892 Security Functions are listed and described in [ST_M7892]:

- **SF_DPM** Device Phase Management
- **SF_PS** Protection against Snooping
- **SF_PMA** Protection against Modification Attacks
- **SF_PLA** Protection against Logical Attacks
- **SF_CS** Cryptographic Support

9.3. MAPPING BETWEEN SFRS AND TOE SECURITY FUNCTIONS

Security Functional Requirement	Coverage by TSS Security Function(s)
FCS_CKM.1/DH_PACE(DH)	SF.CRYPTO
FCS_CKM.1/DH_PACE(ECDH)	SF.CRYPTO
FCS_COP.1/SHA	SF.CRYPTO
FCS_COP.1/SIG_VER	SF.CRYPTO
FCS_COP.1/PACE_ENC	SF.CRYPTO, SF_CS
FCS_COP.1/PACE_MAC	SF.CRYPTO, SF_CS
FCS_CKM.4	SF.CRYPTO
FCS_RND.1	SF.CRYPTO, SF_CS
FIA_AFL.1/Suspend_PIN	SF.PIN_PUK
FIA_AFL.1/Block_PIN	SF.PIN_PUK
FIA_API.1/CA	SF.AUTH
FIA_API.1/RI	SF.AUTH
FIA_UID.1/PACE	SF.AUTH
FIA_UID.1/EAC2_Terminal	SF.AUTH
FIA_UAU.1/PACE	SF.AUTH
FIA_UAU.1/EAC2_Terminal	SF.AUTH
FIA_UAU.4/PACE	SF.AUTH
FIA_UAU.5/PACE	SF.AUTH
FIA_UAU.6/CA	SF.AUTH
FIA_AFL.1/PACE	SF.PIN_PUK
FIA_UAU.6/PACE	SF.AUTH
FDP_ACC.1/TRM	SF.AC, SF_PLA
FDP_ACF.1/TRM	SF.AC, SF_PLA
FDP_RIP.1	SF.CRYPTO, SF.PIN_PUK
FDP_UCT.1/TRM	SF.SM
FDP_UIT.1/TRM	SF.SM
FTP_ITC.1/PACE	SF.SM
FTP_ITC.1/CA2	SF.SM
FAU_SAS.1	SF.MANUFACT_PERSO
FMT_SMF.1	SF.MANUFACT_PERSO, SF.PIN_PUK
FMT_SMR.1/PACE	SF.MNGT
FMT_MTD.1/CVCA_INI	SF.MANUFACT_PERSO
FMT_MTD.1/CVCA_UPD	SF.MNGT
FMT_MTD.1/DATE	SF.MNGT
FMT_MTD.1/PA	SF.MANUFACT_PERSO
FMT_MTD.1/SK_PICC	SF.MANUFACT_PERSO
FMT_MTD.1/KEY_READ	SF.CRYPTO, SF.PIN_PUK
FMT_MTD.1/Initialize_PIN	SF.MANUFACT_PERSO
FMT_MTD.1/Resume_PIN	SF.PIN_PUK
FMT_MTD.1/Change_PIN	SF.PIN_PUK
FMT_MTD.1/Unblock_PIN	SF.PIN_PUK
FMT_MTD.1/Activate_PIN	SF.PIN_PUK
FMT_MTD.3	SF.MNGT
FMT_LIM.1	SF_DPM
FMT_LIM.2	SF_DPM
FMT_MTD.1/INI_ENA	SF.MANUFACT_PERSO
FMT_MTD.1/INI_DIS	SF.MANUFACT_PERSO
FPT_EMS.1	SF.REL
FPT_FLS.1	SF.REL, SF_PMA
FPT_TST.1	SF.REL, SF_PMA
FPT_PHP.3	SF_PMA

© Copyright Thales

END OF DOCUMENT