

# **ID&T**RUST

## **IDENTITY APPLET V3.4/EIDAS**

# ELECTRONIC IDENTITY CARD WITH PACE-GM, PACE-CAM, EXTENDED ACCESS CONTROL V1

## AND V2, RESTRICTED IDENTIFICATION AND ACTIVE

# AUTHENTICATION

# SECURITY TARGET

# COMMON CRITERIA / ISO 15408

# EAL4+

2020

Classification: Public © Copyright ID&Trust Ltd.



## **Revision history**

Version	Date	Information
V1.00	18.08.2020	Final version
V1.01	16.09.2020	Minor modification
V1.02	13.10.2020	Update references



### **Table of Contents**

1	1. ST INTR	RODUCTION	
2	1.1. ST	REFERENCE	8
3	1.2. TO	E Reference	8
4	1.3. TO	E Overview	9
5	1.3.1.	ТОЕ Түре	9
6	1.3.2.	TOE DEFINITION AND OPERATIONAL USAGE	10
7	1.3.3.	TOE MAJOR SECURITY FEATURES FOR OPERATIONAL USE	12
8	1.3.4.	NON-TOE HARDWARE/SOFTWARE/FIRMWARE	12
9	1.4. TO	E DESCRIPTION	14
10	1.4.1.	PRODUCT TYPE	14
11	1.4.2.	COMPONENTS OF THE TOE	15
12	1.4.3.	TOE LIFE CYCLE	18
13	1.4.4.	TOE SECURITY FUNCTIONS	20
14	1.4.5.	FEATURES OF THE IDENTITY APPLET	21
15	2. CONFOR	RMANCE CLAIMS	33
16	2.1. CC	Conformance Claim	33
17	2.2. PP	Claim	33
18	2.3. Pa	ckage Claim	35
19	2.4. Co	nformance Rationale	36
20	2.5. Sta	atement of Compatibility	38
21	2.5.1.	SECURITY FUNCTIONALITIES	38
22	2.5.2.	OSPs	39
23	2.5.3.	SECURITY OBJECTIVES	39
24	2.5.4.	SECURITY REQUIREMENTS	44
25	2.5.5.	ASSURANCE REQUIREMENTS	54
26	2.6. An	alysis	54

27	3. Securi	TY PROBLEM DEFINITION	55
28	3.1. Intr	roduction	55
29	3.1.1.	ASSETS	55
30	3.1.2.	SUBJECTS	57
31	3.2. Thi	reats	60
32	3.2.1.	THREATS FROM EAC1PP	61
33	3.2.2.	THREATS FROM EAC2PP	61
34	3.2.3.	THREATS FROM PACEPP	61
35	3.2.4.	THREATS FROM SSCDPP	62
36	3.3. Orę	ganizational Security Policies	62
37	3.3.1.	OSPS FROM EAC1PP	62
38	3.3.2.	OSPS FROM EAC2PP	63
39	3.3.3.	OSPS FROM PACEPP	63
40	3.3.4.	OSPS FROM SSCDPP	63
41	3.3.5.	ADDITIONAL OSPS	64
42	3.4. Ass	sumptions	65
43	3.4.1.	ASSUMPTIONS FROM EAC1PP	65
44	3.4.2.	ASSUMPTIONS FROM EAC2PP	65
45	3.4.3.	ASSUMPTIONS FROM PACEPP	65
46	3.4.4.	ASSUMPTIONS FROM SSCDPP	65
47	4. SECURI	TY OBJECTIVES	66
48	4.1. See	curity Objectives for the TOE	66
49	4.1.1.	SECURITY OBJECTIVES FOR THE TOE FROM EAC1PP	66
50	4.1.2.	SECURITY OBJECTIVES FOR THE TOE EAC2PP	67
51	4.1.3.	SECURITY OBJECTIVES FOR THE TOE PACEPP	67
52	4.1.4.	SECURITY OBJECTIVES FOR THE TOE SSCDPP	68
53	4.1.5.	ADDITIONAL SECURITY OBJECTIVES FOR THE TOE	69
54	4.2. Se	curity Objectives for the Operational Environment	69

55	4.2.1.	SECURITY OBJECTIVES FROM EAC1PP	69
56	4.2.2.	SECURITY OBJECTIVES FROM EAC2PP	69
57	4.2.3.	SECURITY OBJECTIVES FROM PACEPP	70
58	4.2.4.	SECURITY OBJECTIVES FROM SSCDPP	70
59	4.2.5.	ADDITIONAL SECURITY OBJECTIVES FOR THE ENVIRONMENT	70
60	4.3. Se	curity Objective Rationale	71
61	5. EXTEND	ED COMPONTENTS DEFINITION	75
62	6. SECURI	TY REQUIREMENTS	76
63	6.1. Se	curity Functional Requirements	77
64	6.1.1.	Class FCS	78
65	6.1.2.	Class FIA	96
66	6.1.3.	Class FDP	115
67	6.1.4.	Class FTP	130
68	6.1.5.	Class FAU	133
69	6.1.6.	Class FMT	133
70	6.1.7.	Class FPT	158
71	6.2. Se	curity Assurance Requirements for the TOE	165
72	6.3. Se	curity Requirements Rationale	166
73	6.3.1.	Security Functional Requirements Rationale	166
74	6.3.2.	Rationale for SFR's Dependencies	170
75	6.3.3.	Security Assurance Requirements Rationale	170
76	6.3.4.	Security Requirements – Internal Consistency	171
77	7. TOE SU	JMMARY SPECIFICATION	173
78	7.1. TO	E Security Functions	173
79	7.1.1.	TSF.AccessControl	173
80	7.1.2.	TSF.Authenticate	174
81	7.1.3.	TSF.SecureManagement	177
82	7.1.4.	TSF.CryptoKey	178

83	7.1.5. TSF.AppletParametersSign	
84	7.1.6. TSF.Platform	
85	7.2. Assurance Measures	
86	7.3. Fulfillment of the SFRs	
87	7.4. Correspondence of SFR and TOE mechanis	ms187
88	8. GLOSSARY AND ABBREVIATIONS	
89	9. BIBLIOGRAPHY	
90		



### List of Tables

91	Table 1 Overview of identifiers of current ST and PPs	9
92	Table 2 IDentity Applet Suite v3.4 functionalities       1	0
93	Table 3 Terminals and access control in European Passport	2
94	Table 4 Terminals and access control in Identity Card with Protected MRTD Application2	5
95 96	Table 5 Terminals and access control in Identity Card with EU-compliant MRTD Applicatio	
97	Table 6 Classification of Platform-TSFs	9
98	Table 7 Mapping of security objectives for the TOE    4	3
99	Table 8 Mapping of Security requirements    5	3
100	Table 9 Security Objective Rationale	2
101	Table 10 Overview of authentication and identification SFRs         9	6
102	Table 11 Coverage of Security Objectives for the TOE by SFRs16	7
103	Table 12 Assurance measures and corresponding documents	3



### 104 **1. ST INTRODUCTION**

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

108 **1.1. ST REFERENCE** 

109	Title:	Security Target ID&Trust IDentity Applet v3.4/eIDAS - Electronic		
110		Identity Card with PACE-GM, PACE-CAM, Extended Access		
111		Control v1 and v2, Restricted Identification and Active		
112		Authentication		
113	TOE:	IDentity Applet v3.4/eIDAS on NXP JCOP 4 P71		

- 114 Author: ID&Trust Ltd.
- 115Version Number:v1.02
- 116 Date: 13.10.2020

#### 117 **1.2.TOE Reference**

118 The Security Target refers to the product "ID&Trust IDentity Applet Suite v3.4" for CC 119 evaluation.

- 120 TOE Name: IDentity Applet v3.4/eIDAS on NXP JCOP 4 P71
- 121 TOE short name: IDentity Applet v3.4/eIDAS

122 TOE Identification

- 123 Data: IDentity Applet/eIDAS v3.4.7470
- 124 Evaluation Criteria: [4]
- 125 Evaluation
- 126 Assurance Level: EAL EAL4 augmented with ALC\_DVS.2, ATE\_DPT.2 and
- 127 AVA\_VAN.5 as defined in [3].
- 128 Developer: ID&Trust Ltd.





129 Evaluation Sponsor: NXP Semiconductors Netherlands B.V. 5656, AG Eindhoven, High
130 Tech Campus 60

### **131 1.3.TOE Overview**

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

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

136

Table 1 Overview of identifiers of current ST and PPs

#### 137 1.3.1. TOE TYPE

138 IDentity Applet Suite v3.4 is a highly configurable eID solution. It is able to satisfy multiple

different application requirements even within a single applet instance. The Application part of

the TOE, the applet functionalities are distributed according to the following table:

Application	Function	Standard	Protection Profile (certified or in progress)
IDentity/PKI	Flexible PKI token	CEN TS 14890-1/2 IAS-ECC 1.0.1 [30]	-
IDentity/IAS	European card for e- Services and National e- ID applications	CEN/TS 15480- IAS-ECC 1.0.1 [30]	-
IDentity/QSCD	Qualified Signature Creation Device	CEN/TS 15480-2 IAS-ECC 1.0.1 [30] REGULATION (EU) No 910/2014 BSI TR-03117	[14] [15]
IDentity/IDL	International Driving License	ISO/IEC 18013	-



IDentity/EDL	European Driving	2012/383/EC	-
IDentity/eVR	License Electronic Vehicle Registration	1999/37/EC	-
IDentity/eHC	Electronic Health Insurance	CEN/CWA 15794	-
IDentity/BAC	Basic Access Control (BAC)	ICAO Doc 9303 [8]	BSI-CC-PP-0055
IDentity-J	Basic Access Control (BAC) Password Authenticated Connection Establishment (PACE)	ICAO Doc 9303 [8]	JISEC500 [32] JISEC499 [33]
IDentity/PACE- EAC1	Password Authenticated Connection Establishment (PACE) Extended Access Control v1 (EAC1)	ICAO Doc 9303 [8] ICAO TR-SAC [7] BSI TR-03110 v2.21 [16][17][18][19]	BSI-CC-PP-0068- V2-2011 [13] BSI-CC-PP-0056- V2-2012 [5]
IDentity/eIDAS	Password Authenticated Connection Establishment (PACE) Extended Access Control v2 (EAC2)	ICAO TR-SAC [7] BSI TR-03110 v2.21 [16][17][18][19]	BSI-CC-PP-0087 [20]
	Table 2 Deptity App	let Suite v3 4 functionalities	

 Table 2 IDentity Applet Suite v3.4 functionalities

142 All the functions are supplied by the applet "IDentity Applet Suite v3.4", the behaviour of the

143 applet changes according to the configuration applied during the personalization phase of

144 IDentity Applet life cycle and the environmental behaviour of the usage phase.

# The scope of the current ST is only concerned with applet behaviour of configuration IDentity Applet/elDAS.

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

#### 151 1.3.2. TOE DEFINITION AND OPERATIONAL USAGE

The Target of Evaluation (TOE) is a smartcard programmed according to [16] [17]. The smartcard contains multiple applications (at least one). The programmed smartcard is called an electronic document as a whole. Here, an application is a collection of data(groups) and their access conditions. We mainly distinguish between common user data, and sensitive user-



data. Depending on the protection mechanisms involved, these user data can further bedistinguished as follows:

- EAC1-protected data: Sensitive User Data protected by EAC1 (cf. [16]),
- EAC2-protected data: Sensitive User Data protected by EAC2 (cf. [17]), and
- 160 all other (common) user data: Other user data are protected by Password Authenticated
- 161 Connection Establishment (PACE, cf. also [17]). Note that EAC1 recommends, and EAC2
- 162 requires prior execution of PACE.
- 163 1. Application note (taken from [20], application note 1.)

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

- 169 In addition to the above user data, there are also data required for TOE security functionality
- 170 (TSF). Such data is needed to execute the access control protocols, to verify integrity and
- authenticity of user data, or to generate cryptographic signatures.
- 172 Application considered in [16] and [17] are
- 173 1. an electronic passport (ePass) application
- 174 2. an electronic identity (eID) application, and
- 175 3. a signature (eSign) application.
- 176 The TOE shall comprise at least:
- the circuitry of the chip, including all integrated circuit (IC) dedicated software that is
   active in the operational phase of the TOE,
- 179 2. the IC embedded software, i.e. the operating system,
- 180 3. all access mechanisms, associated protocols and corresponding data,
- 181 4. one or several applications, and
- 182 5. the associated guidance documentation.
- 183 2. Application note (taken from [20], application note 2)

184 Since contactless interface parts (e.g. the antenna) may impact specific aspects of vulnerability

assessment and are thus relevant for security, such parts might be considered as a part of the

186 TOE. The decision upon this is up to the certification body in charge that defines the evaluation

187 methodology for the assessment of the contactless interface.



- 188 1.3.3. TOE MAJOR SECURITY FEATURES FOR OPERATIONAL USE 189 The following TOE security features are the most significant for its operational use: 190 The TOE ensures that 191 only authenticated terminals can get access to the User Data stored on the TOE and 192 use security functionality of the electronic document according to the access rights of 193 the terminal, • the Electronic Document Holder can control access by consciously presenting his 194 195 electronic document and/or by entering his secret PIN, 196 authenticity and integrity of user data can be verified, confidentiality of user data in the communication channel between the TOE and the 197 198 connected terminal is provided, 199 inconspicuous tracing of the electronic document is averted, 200 its security functionality and the data stored inside are self-protected, and 201 digital signatures can be created, if the TOE contains an eSign application. 202 Optionally support the Active Authetnication and Chip Authentication mapping.
- 203 1.3.4. Non-TOE HARDWARE/SOFTWARE/FIRMWARE

In order to be powered up and to communicate with the external world, the TOE needs a terminal (card reader) supporting the communication according to [12] and [11]; the latter only if the card has a contactless interface. Akin to [16] and [17] the TOE shall be able to recognize the following terminal types:

### 208 PACE terminal

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

213 For more information see: PACE Terminal

### 214 EAC1 terminal

An EAC1 terminal is an extended inspection system according to [16]. It performs the advanced inspection procedure ([16]) using EAC1, i.e. PACE, then Chip Authentication 1 followed by Passive Authentication, and finally Terminal Authentication 1. Afterwards user data



- are read by the terminal. An EAC1 terminal is allowed to read both EAC1 protected data, and
- common user data.
- 220 For more information see: EAC1 Terminal / EAC2 Terminal
- EAC2 terminal

An EAC2 terminal is an extended inspection system performing the general authentication procedure according to [17] using EAC2, i.e. PACE, then Terminal Authentication 2 followed by Passive Authentication, and finally Chip Authentication 2. Depending on its authorization level, an EAC2 terminal is allowed to read out some or all EAC2 protected Sensitive User Data, and common user data.

227 For more information see: EAC1 Terminal / EAC2 Terminal

In general, the authorization level of a terminal is determined by the effective terminal authorization. The authorization is calculated from the certificate chain presented by the terminal to the TOE. It is based on the Certificate Holder Authorization Template (CHAT). A CHAT is calculated as an AND-operation from the certificate chain of the terminal and the electronic document presenter's restricting input at the terminal. The final CHAT reflects the effective authorization level and is then sent to the TOE [18]. For the access rights, cf. also the SFR component FDP\_ACF.1/TRM in Chapter 6.1.3.

All necessary certificates of the related public key infrastructure – Country Verifying
 Certification Authority (CVCA) Link Certificates, Document Verifiers Certificates and Terminal
 Certificates – must be available in the card verifiable format defined in [18].

- The term terminal within this ST usually refers to any kind of terminal, if not explicitly mentionedotherwise.
- The current TOE knows three different configuration as described in 1.4.5 Features of the IDentity Applet. According to the each configuration the following tables give an overview which of the above terminals are related to what application, and which data group is accessible.

243	European Passport config	juration		
	<b>Terminal/Application</b>	ePassport	elD	eSign
	PACE terminal	Common user data	n.a.	n.a.
	EAC1 terminal	Common user data and EAC1 protected data	n.a.	n.a.
	EAC2 terminal	none	n.a.	n.a.

### Page 13 of 191



#### 244 Identity Card with Protected MRTD Application configuration

Terminal/Application	ePassport	elD	eSign
PACE terminal	none	none	none
EAC1 terminal	none	none	none
EAC2 terminal	EAC2 protected	· · ·	EAC2 protected data
	data	data	

#### 245 Identity Card with EU-compliant MRTD Application configuration

<b>Terminal/Application</b>	ePassport	elD	eSign
PACE terminal	Common user data	None	None
EAC1 terminal	Common user data and EAC1 protected data	None	None
EAC2 terminal	none	common user data EAC2 protected data	EAC2 protected data

Other terminals than the above are out of scope of this ST. In particular, terminals using Basic

Access Control (BAC) may be functionally supported by the electronic document, but if the TOE is operated using BAC, it is not in a certified mode.

249 **1.4. TOE DESCRIPTION** 

#### 250 1.4.1. PRODUCT TYPE

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

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

257 The TOE type defined both in [5] and [6] is a smartcard. Whereas [5] references [16] (and also 258 [8] and related ICAO specifications, however [16] is fully compatible with those ICAO 259 specifications, and they are mostly listed there for the sake of completeness and the context 260 of use) w.r.t. programming of the card, [17] is given as a reference in [6]. Reference [16] defines 261 the EAC1 protocol, whereas EAC2 is defined in [17]. Thus, this difference in reference is 262 introduced just due to different applications on the card, that do not contradict each other. The 263 term 'travel document' of [5] is here understood in a more broader sense (cf. also Table 1), 264 since the document can also be used in contexts other than just traveling.

The TOE type definition given in [14] is "a combination of hardware and software configured to securely create, use and manage signature-creation data (SCD)". The definition of hardware and software in this ST is more specific by explicitly mentioning a smartcard and the software on the card. However, the very fundamental purpose of a smartcard is to store data on it in a protected way. Hence, the TOE type definition of this ST is also not inconsistent with the one of [14].

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

Operational use of the TOE is explicitly in the focus of [20]. Nevertheless, some TOE functionality might not be directly accessible to the end-user during operational use. Some single properties of the manufacturing and the card issuing life cycle phases that are significant for the security of the TOE in its operational phase are also considered by the current ST. Conformance with [20] requires that all life cycle phases are considered to the extent that is required by the assurance package chosen here for the TOE; c.f. also chapter 6.2

283 1.4.2. COMPONENTS OF THE TOE

#### 284 Micro Controller

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

#### 292 IC dedicated software – Micro Controller Firmware

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

#### 296 IC dedicated software – Crypto Library



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

Micro Controller, IC dedicated software (Micro Controller Firmware, Crypto Library) are covered by the following certification: Certification ID: BSI-DSZ-CC-1040-2019-MA-01

Evaluation level EAL6+ ALC\_FLR.1 and ASE\_TSS.2 according to Security IC Platform
Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-000842014.

#### 307 IC Embedded Software

308 Certification ID: NSCIB-CC-180212-CR2

309 JCOP4 consists of Java Card Virtual Machine (JCVM), Java Card Runtime Environment

310 (JCRE), Java Card API (JCAPI), Global Platform (GP) framework, Configuration Module, etc.

- 311 OS Name: JCOP 4 Operating System 312 Applied OS 313 configuration: Banking & Secure ID 314 315 Product Identification: JCOP 4 v4.7 R1.00.4 316 317 Evaluation Level: CC EAL 6+ with ASE TSS.2, ALC FLR.1 according to Java Card 318 319 System – Open Configuration Protection Profile, version 3.0.5, Certified 320 by Bundesamt für Sicherheit in der Informationstechnik (BSI, BSI-CC-321 PP-0099-2017). 322 Platform UGD: [24] 323 ID&Trust IDentity Applet Suite – accomplishing IDentity Applet v3.4/eIDAS 324 Product name: ID&Trust IDentity Applet Suite 325 Version: 3.4
- 326 Application name<sup>1</sup>: IDentity Applet v3.4/eIDAS
- 327 TOE Guidance

<sup>&</sup>lt;sup>1</sup> The applet is provided in cap file format.



- 328 Documentation: <sup>2</sup> IDentity Applet Administrator's Guide [21]
- 329IDentity Applet User's Guide [22]
- 330 The composite part always means IDentity Applet v3.4/eIDAS
- 331 The logical architecture of the TOE:



#### 1. Figure TOE Boundaries

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

The blue box marks the application layer. The ID&Trust IDentity Applet Suite v3.4 could be loaded in the Flash. During the creation phase an instance is created in the Flash and after several configuration steps it will be personalized as IDentity Applet v3.4/eIDAS. For details please see: section 1.4.3 TOE life cycle and [23].

<sup>&</sup>lt;sup>2</sup> The AGD documents provided in electronic document format.

341 The boxes marked with white are not certified.

#### 342 1.4.3. TOE LIFE CYCLE

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

- 345 **Phase 1: Development**
- 346 Step 1
- The TOE is developed in phase 1. NXP develops the integrated circuit, the IC dedicated software and the guidance documentation associated with these TOE components.
- 349 Step 2

The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC dedicated software, and develops the IC embedded software (operating system), the electronic document application(s) and the guidance documentation associated with these TOE components. The operating system is developed by NXP as well. The IDentity Applet v3.4 is developed by ID&Trust Ltd.

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

#### 360 Phase 2: Manufacturing

361 Step 3

362 In a first step, the TOE integrated circuit is produced. The circuit contains the electronic 363 document's chip dedicated software, and the parts of the electronic document's chip 364 embedded software in the non-volatile non-programmable memory (ROM). The IC 365 manufacturer writes IC identification data onto the chip in order to track and control the IC as 366 dedicated electronic document material during IC manufacturing, and during delivery to the 367 electronic document manufacturer. The IC is securely delivered from the IC manufacturer to 368 the electronic document manufacturer. If necessary, the IC manufacturer adds parts of the IC 369 embedded software in the non-volatile programmable memory, e. g. EEPROM or in FLASH.

- 370 Step 4 (optional)
- 371 If the electronic document manufacturer delivers a packaged component, the IC is combined372 with hardware for the contact based or contactless interface.
- 373 Step 5
- 374 The electronic document manufacturer
- if necessary, adds the IC embedded software, or parts of it in the non-volatile
   programmable memories, e. g. EEPROM or FLASH,
- 377 2. creates the application(s), and
- 378 3. equips the electronic document's chip with pre-personalization data.

379 Creation of the application(s) implies the creation of the master file (MF), dedicated files (DFs), 380 and elementary files (EFs) according to [12]. How this process is handled internally depends 381 on the IC and IC embedded software.

- The pre-personalized electronic document together with the IC identifier is securely delivered from the electronic document manufacturer to the Personalization Agent. The electronic document manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.
- 386 Phase 3: Personalization of the Electronic Document
- 387 Step 6
- 388 The personalization of the electronic document includes
- 389 1. the survey of the Electronic Document Holder's biographical data,
- the enrollment of the Electronic Document Holder's biometric reference data, such as
   a digitized portrait or other biometric reference data,
- 392 3. printing the visual readable data onto the physical part of the electronic document, and
- 393 4. configuration of the TSF, if necessary.

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

- 399 3. Application note (taken from [20], Application Note 3)
- TSF data are data for the operation of the TOE upon which the enforcement of the SFRs relies
  [1]. Here TSF data include, but are not limited to, the Personalization Agent's authentication
  key(s).
- 403 **Phase 4: Operational Use**
- 404 Step 7
- 405 The chip of the TOE is used by the electronic document and terminals that verify the chip's
- 406 data during the phase operational use. The user data can be read and modified according to
- 407 the security policy of the issuer.
- 408 4. Application note (taken from [20], application note 4)

This ST considers at least the first phase and parts of the second phase, i.e. Step 1 up to Step 3, as part of the evaluation. Therefore, the TOE delivery is defined to occur, according to CC, after Step 3. Since specific production steps of the second phase are of minor security relevance (e.g. plastic card or booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless, the decision about this has to be taken by the certification body resp. the national body of the issuer or organization. In this case the national body of the issuer is responsible for these specific production steps.

Note that the personalization process and its environment may depend on specific security needs of the issuer. All production, generation and installation procedures after TOE delivery up to the phase operational use have to be considered in the product evaluation process under assurance class AGD. Therefore, the security target has to outline how to split up P.Manufact, P.Personalisation and related security objectives into aspects relevant before vs. those relevant after TOE delivery.

- 422 Some production steps, e. g. Step 4 in Phase 2 may also take place in the Phase 3.
- 423 1.4.4. TOE SECURITY FUNCTIONS

TSF	Description
TSF.AccessControl	The TOE enforces access control in order to ensure only for authorised users to access User Data and TSF-data and maintains different security roles.
TSF.Authenticate	The TOE supports several authentication mechanisms in order to authenticate the Users, Terminals and to prove the genuineness of the electronic document. The supported mechanism and protocols are based on ICAO and BSI standards [7], [8], [16], [17] and [18].
TSF.SecureManagement	The TOE enforces the secure management of the security attributes, data and functions. Furthermore the TOE restricts the available commands in each TOE life-cycle phase.
TSF.CryptoKey	The TOE uses several cryptographic services such as digital signature creation and verification, asymmetric and

	symmetric cryptography, random number generation and complete key management.
TSF.AppletParametersSign	The TOE enforces the integrity of itself in each life cycle phases.
TSF.Platform	The TOE relies on the certified functions and services of the Platform. This TSF is collection of those SFRs, which are uses these functions and services.

#### 424 1.4.5. FEATURES OF THE IDENTITY APPLET

- 425 Taking into consideration the [20] the current ST makes distinct the following configuration:
- 426 European Passport
- Identity Card with Protected MRTD Application
- Identity Card with EU-compliant MRTD Application
- 429 1.4.5.1. European Passport
- 430 Passwords
- 431 MRZ [16]
- 432 CAN [16]
- 433 Authentication Procedure
- This configuration requires implementation t the following Authentication Procedure for access
  to DG3 and DG4 (Sensitive User Data) of the ePassport Application:
- Advanced Inspection procedure [16]
- 437 Applications
- ePassport Application
- 439 Protocols
- PACE (Generic Mapping, Integrated Mapping and Chip Authentication Mapping) [9],
   [16]
- Active Authentication [7] (optionally)
- 443 EAC1 [16]
- 444 o Terminal Authentication version 1 [16]
- 445 o Chip Authentication version 1 [16]
- 446 Data Groups
- 447 According to [16].
- 448 Data types in:



- Common user data: All DG, which require only BAC/PACE protocol
- EAC1 protected data: All DG, which require EAC1 protocol
- 451 The authorization level of EAC1 terminal is determined by the effective authorization calculated452 by from the certificate chain.
- 453 Terminals and access control

PACE terminal	EAC1 terminal	EAC2 terminal
Х	Х	-
-	Х	-
	PACE terminal	PACE terminalEAC1 terminalXX-X

Table 3 Terminals and access control in European Passport

#### 455 Security Functional Requirements

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



FIA_AFL.1/PACE_EAC2PP	-
FIA_UAU.6/PACE_EAC2PP	-
FIA_UID.1/PACE_EAC1PP	Х
FIA_UAU.1/PACE_EAC1PP	Х
FIA_UAU.4/PACE_EAC1PP	Х
FIA_UAU.5/PACE_EAC1PP	Х
FIA UAU.6/PACE EAC1PP	Х
FIA UAU.6/EAC EAC1PP	Х
FIA_API.1/EAC1PP	Х
FIA API.1/PACE CAM	Х
FIA API.1/AA	Х
FIA AFL.1/PACE EAC1PP	X
FIA UID.1/SSCDPP	-
FIA AFL.1/SSCDPP	_
FIA UAU.1/SSCDPP	
FDP ACC.1/TRM EAC2PP	
FDP_ACF.1/TRM	X
FDP_ACF.I/IRM FDP_RIP.1/EAC2PP	
	-
FDP_UCT.1/TRM_EAC2PP	-
FDP_UIT.1/TRM_EAC2PP	-
FDP_ACC.1/TRM_EAC1PP	<u>X</u>
FDP_RIP.1/EAC1PP	X
FDP_UCT.1/TRM_EAC1PP	X
FDP_UIT.1/TRM_EAC1PP	X
FDP_ACC.1/SCD/SVD_Generation_S	-
SCDPP	
FDP_ACF.1/SCD/SVD_Generation_S	-
SCDPP	
FDP_ACC.1/SVD_Transfer_SSCDPP	-
FDP_ACF.1/SVD_Transfer_SSCDPP	-
FDP_ACC.1/Signature-	-
creation_SSCDPP	
FDP_ACF.1/Signature-	-
creation_SSCDPP	
FDP_RIP.1/SSCDPP	-
FDP_SDI.2/Persistent_SSCDPP	-
FDP_SDI.2/DTBS_SSCDPP	-
FTP_ITC.1/PACE_EAC2PP	-
FTP_ITC.1/CA_EAC2PP	-
FTP_ITC.1/PACE_EAC1PP	Х
FAU_SAS.1/EAC2PP	-
FAU_SAS.1/EAC1PP	Х
FMT_MTD.1/CVCA_INI_EAC2PP	<u>-</u>
FMT_MTD.1/CVCA_UPD_EAC2PP	-
FMT_SMF.1/EAC2PP	-
FMT_SMR.1	Х
FMT_MTD.1/DATE_EAC2PP	-
FMT_MTD.1/PA_EAC2PP	
FMT_MTD.1/SK_PICC_EAC2PP	
FMT_MTD.1/KEY_READ_EAC2PP	
	-
FMT_MTD.1/Initialize_PIN_EAC2PP	-
FMT_MTD.1/Change_PIN_EAC2PP	-
FMT_MTD.1/Resume_PIN_EAC2PP	-
FMT_MTD.1/Unblock_PIN_EAC2PP	-
FMT_MTD.1/Activate_PIN_EAC2PP	-



FMT_MTD.3/EAC2PP	-
FMT_SMR.1/SSCDPP	-
FMT_SMF.1/SSCDPP	-
FMT_MOF.1/SSCDPP	-
FMT_MSA.1/Admin_SSCDPP	-
FMT_MSA.1/SignatorySSCDPP	-
FMT_MSA.2/SSCDPP	-
FMT_MSA.3/SSCDPP	-
FMT_MSA.4/SSCDPP	-
FMT_MTD.1/Admin_SSCDPP	-
FMT_MTD.1/Signatory_SSCDPP	-
FMT_LIM.1/EAC2PP	-
FMT_LIM.2/EAC2PP	-
FMT_MTD.1/INI_ENA_EAC2PP	-
FMT_MTD.1/INI_DIS_EAC2PP	-
FMT_SMF.1/EAC1PP	Х
FMT_LIM.1/EAC1PP	Х
FMT_LIM.2/EAC1PP	Х
FMT_MTD.1/INI_ENA_EAC1PP	Х
FMT_MTD.1/INI_DIS_EAC1PP	Х
FMT_MTD.1/CVCA_INI_EAC1PP	Х
FMT_MTD.1/CVCA_UPD_EAC1PP	Х
FMT_MTD.1/DATE_EAC1PP	Х
FMT_MTD.1/CAPK_EAC1PP	Х
FMT_MTD.1/PA_EAC1PP	Х
FMT_MTD.1/KEY_READ_EAC1PP	Х
FMT_MTD.3/EAC1PP	Х
FMT_LIM.1/Loader	Х
FMT_LIM.2/Loader	Х
FMT_MTD.1/AA_Private_Key	Х
FPT_EMS.1/EAC2PP	-
FPT_FLS.1/EAC2PP	-
FPT_TST.1/EAC2PP	-
FPT_PHP.3/EAC2PP	-
FPT_TST.1/EAC1PP	Х
FPT_FLS.1/EAC1PP	Х
FPT_PHP.3/EAC1PP	Х
FPT_EMS.1/EAC1PP	Х
FPT_EMS.1/SSCDPP	-
FPT_FLS.1/SSCDPP	-
FPT_PHP.1/SSCDPP	_
FPT_PHP.3/SSCDPP	_
FPT_TST.1/SSCDPP	

1.4.5.2. Identity Card with Protected MRTD Application

- 457 Passwords
- 458 MRZ [16]
- 459 CAN [16]
- 460 PIN [17]



461 • PUK [17]

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

466 Authentication Procedure

467 This configuration requires implementation at the following Authentication Procedure for 468 access any User Data stored on the TOE:

- General Authentication Procedure [17]
- 470 Applications
- ePassport Application
- eID Application
- eSign Application
- 474 Protocols
- PACE (Generic Mapping, Integrated Mapping) [17]
- 476 EAC2 [17]
- 477 o Terminal Authentication version 2 [17]
- 478 Chip Authentication version 2 [17]
- Restricted Identification [17]
- 480 Data Groups
- 481 According to [17].
- 482 According to [9] and [16].
- 483 Data type in:
- EAC2 protected data: All DG in ePassport, eID and eSign application.

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

487 Terminals and access control

Data type	PACE terminal	EAC1 terminal	EAC2 terminal
Common user data	-	-	Х
EAC2 protected data	-	-	Х
Table 4 Terminal	a and access control in I	dontity Cord with Protocto	d MPTD Application

488

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



FCS         CKM.1/DH_PACE_EAC2PP         X         X         X         X           FCS_COP.1/ISIG_VER_EAC2PP         X         X         X         X           FCS_COP.1/ISIG_VER_EAC2PP         X         X         X         X           FCS_COP.1/PACE_MAC_EAC2PP         X         X         X         X           FCS_COP.1/PACE_MAC_EAC2PP         X         X         X         X           FCS_COP.1/PACE_MAC_EAC2PP         X         X         X         X           FCS_COP.1/PACE_EAC1PP         -         -         -         -           FCS_COP.1/PACE_EAC_EAC1PP         -         -         -         -           FCS_COP.1/PACE_MAC_EAC1PP         -         -         -         -           FCS_COP.1/FACE_MAC_EAC1PP         -         -         -         -           FCS_COP.1/CA_MAC_EAC1PP         -         -         -         -           FCS_COM.1/CA_MAC_EAC1PP         -         -         -	TOE SFR / Application	ePassport	elD	eSign
FCS_COP.1/SHA_EAC2PP       X       X       X         FCS_COP.1/IAGE_ENC_EAC2PP       X       X       X         FCS_COP.1/PACE_ENC_EAC2PP       X       X       X         FCS_COP.1/PACE_ENC_EAC2PP       X       X       X         FCS_COP.1/PACE_ENC_EAC2PP       X       X       X         FCS_COP.1/PACE_ENC_EAC1PP       -       -       -         FCS_COP.1/PACE_ENC_EAC1PP       -       -       -         FCS_COP.1/PACE_ENC_EAC1PP       -       -       -         FCS_COP.1/PACE_ENC_EAC1PP       -       -       -         FCS_COP.1/PACE_EAC1PP       -       -       -         FCS_COP.1/FACE_EAC1PP       -       -       -         FCS_COP.1/CAC_ENC_EAC1PP       -       -       -         FCS_COP.1/CAC_EACC_EAC1PP       -       -       -         FCS_COM.1/FACE_EAC1PP       -       -       -         FCS_COM.1/FACE_EAC1PP <t< td=""><td>FCS CKM.1/DH PACE EAC2PP</td><td>Х</td><td>Х</td><td>Х</td></t<>	FCS CKM.1/DH PACE EAC2PP	Х	Х	Х
FCS       COP.1/SIG VER_EAC2PP       X       X       X         FCS       COP.1/PACE_MAC_EAC2PP       X       X       X         FCS       CCN.1/PACE_MAC_EAC2PP       X       X       X         FCS       CKM.4/EAC2PP       X       X       X         FCS       CKM.4/EAC2PP       X       X       X         FCS       CKM.1/DH_PACE_EAC1PP       -       -       -         FCS       CCN.1/PACE_MAC_EAC1PP       -       -       -         FCS       COP.1/PACE_MAC_EAC1PP       -       -       -         FCS       COP.1/PACE_MAC_EAC1PP       -       -       -         FCS       COP.1/FACE_MAC_EAC1PP       -       -       -         FCS       COP.1/CA_MAC_EAC1PP       -       -       -         FCS       CCN.1/CA_MAC_EAC1PP       -       -       -         FCS       CKM.1/CA_AC2       X       X       X       X         FCS       CKM.1/CA_AC2       X       X       X       -       -         FCS       CKM.1/CA_AC1PP       -       -       -       -       -         FCS       CKM.1/CA       AC1PP       -       -				
FCS_COP.1/PACE_ENC_EAC2PP         X         X         X           FCS_COP.1/PACE_MAC_EAC2PP         X         X         X           FCS_CKM.4/EAC2PP         X         X         X           FCS_CKM.4/EAC2PP         X         X         X           FCS_CKM.4/EAC2PP         X         X         X           FCS_CKM.4/EAC1PP         -         -         -           FCS_COP.1/PACE_ENC_EAC1PP         -         -         -           FCS_COP.1/PACE_ENC_EAC1PP         -         -         -           FCS_COP.1/FACE_ENC_EAC1PP         -         -         -           FCS_COP.1/FACE_ENC_EAC1PP         -         -         -           FCS_COP.1/FACE_EAC1PP         -         -         -           FCS_COP.1/CA_ENC_EAC1PP         -         -         -           FCS_COP.1/CA_ENC_EAC1PP         -         -         -           FCS_COP.1/CA_ENC_EAC1PP         -         -         -           FCS_COP.1/CA_ENC_EAC1PP         -         -         -           FCS_COP.1/CA_MAC_EAC1PP         -         -         -           FCS_CON.1/CA_ENC_EAC1PP         -         -         -           FCS_CON.1/CAM         -         -<				
FCS         COP.1/PACE         MAC         EAC2PP         X         X         X           FCS         ROL         IEAC2PP         X         X         X         X           FCS         RND.1/EAC2PP         X         X         X         X           FCS         CKM.1/DH_PACE_EAC1PP         -         -         -           FCS         COP.1/PACE_ENC_EAC1PP         -         -         -           FCS         COP.1/PACE_MAC EAC1PP         -         -         -           FCS         COP.1/PACE_EAC1PP         -         -         -           FCS         COP.1/CA_MAC_EAC1PP         -         -         -           FCS         COP.1/SIG         VER         EAC1PP         -         -           FCS         COP.1/SIG         VER         EAC1PP         -         -         -           FCS         CKM.1/RI         -         X         X         X         -         -           FCS         CKM.1/RA         -         -         -         -         -         -           FCS         CKM.1/RA         -         -         -         -         -         -           FCS				
FCS_CKM.4/EAC2PP         X         X         X         X           FCS_CKM.1/DH_PACE_EAC1PP         -         -         -         -           FCS_CKM.1/DH_PACE_EAC1PP         -         -         -         -           FCS_CKM.1/DH_PACE_EAC1PP         -         -         -         -           FCS_COP.1/PACE_MAC_EAC1PP         -         -         -         -           FCS_COP.1/PACE_MAC_EAC1PP         -         -         -         -           FCS_COP.1/CA_EAC1PP         -         -         -         -           FCS_COP.1/CA_EAC1PP         -         -         -         -           FCS_COP.1/CA_MAC_EAC1PP         -         -         -         -           FCS_COP.1/CA_MAC_EAC1PP         -         -         -         -           FCS_COP.1/CA_MAC_EAC1PP         -         -         -         -           FCS_CKM.1/CA         -         -         -         -         -           FCS_CKM.1/AA         -         -         -         -         -           FCS_CKM.1/AA         -         -         -         -         -           FCS_CKM.1/AA         -         -         -         -         <				
FCS_RND.1/EAC2PP         X         X         X         X           FCS_CKM.1/DH_PACE_EAC1PP         -         -         -         -           FCS_CKM.4/EAC1PP         -         -         -         -           FCS_COP.1/PACE_ENC_EAC1PP         -         -         -         -           FCS_COP.1/PACE_MAC_EAC1PP         -         -         -         -           FCS_CON_1/EAC1PP         -         -         -         -           FCS_COP.1/EAC_ENC_EAC1PP         -         -         -         -           FCS_CON_1/SIG_VER_EAC1PP         -         -         -         -           FCS_CON.1/SIG_VER_EAC1PP         -         -         -         -           FCS_CON.1/SIG_VER_EAC1PP         -         -         -         -           FCS_CON.1/RA         -         -         -         -         -           FCS_CKM.1/RA         -         -         -         -         -         -           FCS_COP.1/CAM         -         -         -         -         -         -         -           FCS_COP.1/SCDPP         -         -         X         X         X         X           FIA_APL1/ROL_EAC2PP				
FCS_CKM.1/DH_PACE_EAC1PP       -       -       -         FCS_COP.1/PACE_ENC_ENC_EAC1PP       -       -       -         FCS_COP.1/PACE_MAC_EAC1PP       -       -       -         FCS_CKM.1/CA_ENC_EAC1PP       -       -       -         FCS_CKM.1/CA_ENC_EAC1PP       -       -       -         FCS_CCP.1/CA_ENC_EAC1PP       -       -       -         FCS_COP.1/CA_ENC_EAC1PP       -       -       -         FCS_COP.1/CA_MC_EAC1PP       -       -       -         FCS_COP.1/CA_MC_EAC1PP       -       -       -         FCS_COP.1/CA_MAC_EAC1PP       -       -       -         FCS_CKM.1/GA2       X       X       X         FCS_CCM.1/AA       -       -       -         FCS_CCM.1/CAM       -       -       -         FCS_CCM.1/SSCDPP       -       -       X         FCS_CCM.1/SSCDPP       -       -       X         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X       X         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X       X         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X       X         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X <t< td=""><td>——————</td><td></td><td></td><td></td></t<>	——————			
FCS_CKM.4/EAC1PP       -       -       -         FCS_COP.1/PACE_MAC_EAC1PP       -       -       -         FCS_COM.1/CAC_EAC1PP       -       -       -         FCS_COP.1/FACE_MAC_EAC1PP       -       -       -         FCS_COP.1/CA_EAC1PP       -       -       -         FCS_COP.1/CA_EAC1PP       -       -       -         FCS_COP.1/CA_MAC_EAC1PP       -       -       -         FCS_COP.1/CA_MAC_EAC1PP       -       -       -         FCS_COM.1/CA2       X       X       X         FCS_COM.1/CA2       X       X       X         FCS_COM.1/CA4       -       -       -         FCS_COM.1/CAM       -       -       -         FCS_COP.1/SCDPP       -       -       X         FCS_COP.1/SCDPP       -       -				
FCS_COP.1/PACE_ENC_EAC1PP       -       -         FCS_COP.1/PACE_MAC_EAC1PP       -       -         FCS_RM.1/CA_EAC1PP       -       -         FCS_COP.1/CA_ENC_EAC1PP       -       -         FCS_COP.1/CA_ENC_EAC1PP       -       -         FCS_COP.1/CA_MAC_EAC1PP       -       -         FCS_COP.1/CA_MAC_EAC1PP       -       -         FCS_CKM.1/RA       -       -         FCS_CKM.1/RA       -       -         FCS_CCM.1/CA       -       -         FCS_CCM.1/AA       -       -         FCS_CCM.1/CAM       -       -         FCS_CCP.1/CAM       -       -         FCS_CCP.1/SSCDPP       -       -         FCS_CCP.1/SSCDPP       -       -         FCS_CCP.1/SSCDPP       -       -         FIA_FL.1/Slock_PIN_EAC2PP       X       X         FIA_APL.1/RL_AC2PP       X       X         FIA_APL.1/RL_AC2PP       X       X         FIA_UD.1/PACE_EAC2PP       <		-		-
FCS_COP.1/PACE_MAC_EAC1PP       -       -         FCS_CNL1/CA_EAC1PP       -       -         FCS_COP.1/CA_ENC_EAC1PP       -       -         FCS_COP.1/CA_ENC_EAC1PP       -       -         FCS_COP.1/CA_ENC_EAC1PP       -       -         FCS_COP.1/CA_MAC_EAC1PP       -       -         FCS_COP.1/CA_MAC_EAC1PP       -       -         FCS_CKM.1/CA2       X       X       X         FCS_CKM.1/CA4       -       -       -         FCS_CCM.1/CAM       -       -       -         FCS_COP.1/AA       -       -       -         FCS_COP.1/CAM       -       -       -         FCS_COP.1/CAM       -       -       -         FCS_COP.1/SSCOPP       -       -       X         FCS_COP.1/SSCOPP       -       -       X         FCS_COP.1/SSCOPP       -       -       X         FCS_COP.1/SSCOPP       -       -       X         FCS_COP.1/SCOPP       -       -       X         FCS_COP.1/SSCOPP       -       -       X         FCS_COP.1/SCOPP       -       -       X         FIA_SCOPP       X       X       X		-	-	-
FCS_RND.1/EAC1PP       -       -       -         FCS_CKM.1/CA_EAC1PP       -       -       -         FCS_COP.1/CA_MAC_EAC1PP       -       -       -         FCS_COP.1/CA_MAC_EAC1PP       -       -       -         FCS_COP.1/CA_MAC_EAC1PP       -       -       -         FCS_CKM.1/CA2       X       X       X       X         FCS_CKM.1/CA1       -       X       -       -         FCS_CCM.1/CAM       -       -       -       -         FCS_COP.1/CAM       -       -       -       -         FCS_COP.1/CAM       -       -       -       -         FCS_COP.1/CAM       -       -       -       -         FCS_COP.1/SSCDPP       -       -       X       X         FLA_AFL_1/Suspend_PIN_EAC2PP       X       X       X       X         FLA_AFL_1/RL_CA_EAC2PP       X       X       X       X         FLA_AFL_1/PACE_EAC2PP <t< td=""><td></td><td>-</td><td>-</td><td>-</td></t<>		-	-	-
FCS_CKM.1/CA_EAC1PP       -       -         FCS_COP.1/CA_ENC_EAC1PP       -       -         FCS_COP.1/CA_MAC_EAC1PP       -       -         FCS_CCN1/CA_MAC_EAC1PP       -       -         FCS_CKM.1/CA2       X       X       X         FCS_CCN1/CA_MAC_EAC1PP       -       -         FCS_CKM.1/CA2       X       X       X         FCS_CKM.1/CA4       -       -       -         FCS_COP.1/CA       -       -       -         FCS_COP.1/CAM       -       -       -         FCS_COP.1/CAM       -       -       -         FCS_COP.1/CAM       -       -       -         FCS_COP.1/SSCDPP       -       -       X         FCS_COP.1/SSCDPP       -       -       X         FCS_COP.1/SSCDPP       -       -       X         FIA_AFL.1/Suspend PIN EAC2PP       X       X       X         FIA_AFL.1/Suspend PIN EAC2PP       X       X       X         FIA_UD1/IPACE EAC2PP       X       X       X         FIA_UD1/IPACE EAC2PP       X       X       X         FIA_UAU.1/PACE EAC2PP       X       X       X         FIA_UAU.1/PACE E		-	-	-
FCS_COP.1/CA_ENC_EAC1PP       -       -         FCS_COP.1/SIG_VER_EAC1PP       -       -         FCS_COP.1/CA_MAC_EAC1PP       -       -         FCS_CKM.1/CA       X       X         FCS_CKM.1/CA       -       -         FCS_CCP.1/CA_MAC_       -       -         FCS_CCP.1/CA       -       -         FCS_CCP.1/CAM       -       -         FCS_COP.1/CAM       -       -         FCS_CCP.1/CAM       -       -         FCS_COP.1/SSCDPP       -       -         FCS_COP.1/SSCDPP       -       -         FCS_CCM.1/SSCDPP       -       -         FCS_CCP.1/SSCDPP       -       -         FCS_CCP.1/SSCDPP       -       -         FCS_CCP.1/SSCDPP       -       -         FCS_CCP.1/SSCDPP       -       -         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X         FIA_APL1/RICA_EAC2PP       X       X         FIA_APL1/REAC2_Terminal_EAC2PP       X       X         FIA_UDU.1/PACE_EAC2PP       X       X         FIA_UAU.1/PACE_EAC2PP       X       X         FIA_UA	—	-	-	-
FCS_COP.1/SIG_VER_EAC1PP       -       -         FCS_CKM.1/CA2       X       X       X         FCS_CKM.1/CA2       X       X       X         FCS_CKM.1/RI       -       X       -         FCS_CCM.1/AA       -       -       -         FCS_CCM.1/AA       -       -       -         FCS_CCM.1/CAM       -       -       -         FCS_CCP.1/CAM       -       -       -         FCS_CCP.1/SSCDPP       -       -       X         FCS_COP.1/SSCDPP       -       -       X         FCS_CCP.1/SSCDPP       -       -       X         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X       X         FIA_APIL.1/Suspend_PIN_EAC2PP       X       X       X         FIA_APIL.1/Block PIN_EAC2PP       X       X       X         FIA_UID.1/PACE_EAC2PP       X       X       X         FIA_UID.1/PACE_EAC2PP       X       X       X         FIA_UUL.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X		-	-	-
FCS_COP.1/CA_MAC_EAC1PP       -       -       -         FCS_CKM.1/Rat       -       X       X       X         FCS_CKM.1/RI       -       X       -         FCS_COP.1/AA       -       -       -         FCS_COP.1/CAM       -       -       -         FCS_COP.1/CAM       -       -       -         FCS_COP.1/CAM       -       -       -         FCS_COP.1/SSCDPP       -       -       X         FCS_COP.1/SSCDPP       -       -       X         FCS_COP.1/SSCDPP       -       -       X         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X       X         FIA_APL.1/RI_EAC2PP       X       X       X         FIA_APL.1/REAC2PP       -       X       -         FIA_UID.1/PACE_EAC2PP       X       X       X         FIA_UUL/IPACE_EAC2PP       X       X       X         FIA_UUL/IPACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UUL/IPACE_EAC2PP       X       X       X         FIA_UUL/IPACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP				-
FCS_CKM.1/CA2       X       X       X         FCS_CKM.1/RI       -       X       -         FCS_CKM.1/AA       -       -       -         FCS_COP.1/AA       -       -       -         FCS_COP.1/CAM       -       -       -         FCS_COP.1/SSCDPP       -       -       X         FCS_COP.1/SSCDPP       -       -       X         FCS_COP.1/SSCDPP       -       -       X         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X       X         FIA_AFL.1/Block_PIN_EAC2PP       X       X       X         FIA_APL.1/RECK2_EAC2PP       X       X       X         FIA_APL.1/RECK2_Terminal_EAC2PP       -       X       X         FIA_UUD.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.5/PACE_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.5/PACE_EA		-	-	
FCS_CKM.1/RI       -       X       -         FCS_CKM.1/AA       -       -       -         FCS_COP.1/AA       -       -       -         FCS_CKM.1/CAM       -       -       -         FCS_COP.1/CAM       -       -       -         FCS_COP.1/SSCDPP       -       -       X         FIA_AFL.1/SUPP       -       -       X         FIA_AFL.1/SUPP       X       X       X         FIA_AFL.1/Block_PIN_EAC2PP       X       X       X         FIA_AFL.1/Block_PIN_EAC2PP       X       X       X         FIA_APL.1/RL_EAC2PP       X       X       X         FIA_DUD.1/FACE_EAC2PP       X       X       X         FIA_UUD.1/FACE_Terminal_EAC2PP       X       X       X         FIA_UAU.1/FACE_EAC2PP       X       X       X         FIA_UAU.3/PACE_EAC2PP		X	X	X
FCS_CKM.1/AA       -       -       -         FCS_COP.1/AA       -       -       -         FCS_CKM.1/CAM       -       -       -         FCS_COP.1/CAM       -       -       -         FCS_COP.1/SSCDPP       -       -       X         FCS_COP.1/SSCDPP       -       -       X         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X       X         FIA_AFL.1/Block_PIN_EAC2PP       X       X       X         FIA_AFL.1/BLCA_EAC2PP       X       X       X         FIA_API.1/CA_EAC2PP       X       X       X         FIA_DUD.1/PACE_EAC2PP       X       X       X         FIA_UUD.1/PACE_EAC2PP       X       X       X         FIA_UUD.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.4/FACE_EAC2PP       X       X       X         FIA_UAU.4/FACE_EAC2PP       X       X       X         FIA_UAU.4/FACE_EAC2PP       X       X       X         FIA_UAU.4/FACE_EAC2PP       X       X       X         FIA_UAU.4/FACE_E				
FCS_COP.1/AA       -       -       -         FCS_CKM.1/CAM       -       -       -         FCS_COP.1/CAM       -       -       -         FCS_COP.1/SSCDPP       -       -       X         FCS_COP.1/SSCDPP       -       -       X         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X       X         FIA_AFL.1/Block_PIN_EAC2PP       X       X       X         FIA_API.1/CA_EAC2PP       X       X       X         FIA_API.1/RL_EAC2PP       -       X       X         FIA_DID.1/FACE_EAC2PP       X       X       X         FIA_UID.1/PACE_EAC2PP       X       X       X         FIA_UUD.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/PAC				
FCS_CKM.1/CAM       -       -       -         FCS_COP.1/CAM       -       -       -         FCS_CCDP.1/SSCDPP       -       -       X         FCS_COP.1/SSCDPP       -       -       X         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X       X         FIA_AFL.1/Block_PIN_EAC2PP       X       X       X         FIA_AFL.1/BLCA_EAC2PP       X       X       X         FIA_API.1/CA_EAC2PP       X       X       X         FIA_DUD.1/PACE_EAC2PP       X       X       X         FIA_UID.1/PACE_EAC2PP       X       X       X         FIA_UID.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.5/PACE_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA	————————			
FCS_COP.1/CAM       -       -       -         FCS_CKM.1/SSCDPP       -       -       X         FCS_COP.1/SSCDPP       -       -       X         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X       X         FIA_AFL.1/Biock_PIN_EAC2PP       X       X       X         FIA_API.1/CA_EAC2PP       X       X       X         FIA_API.1/Ri_EAC2PP       X       X       X         FIA_API.1/Ri_EAC2PP       X       X       X         FIA_UID.1/PACE_EAC2PP       X       X       X         FIA_UID.1/EAC2_Terminal_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.5/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC1PP       -       -       -	————————			
FCS_CKM.1/SSCDPP       -       -       X         FCS_COP.1/SSCDPP       -       -       X         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X       X         FIA_AFL.1/Block_PIN_EAC2PP       X       X       X         FIA_APL.1/CA_EAC2PP       X       X       X         FIA_APL.1/RL_EAC2PP       X       X       X         FIA_APL.1/RL_EAC2PP       -       X       X         FIA_UDL.1/PACE_EAC2PP       X       X       X         FIA_UID.1/PACE_EAC2PP       X       X       X         FIA_UUL.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.5/PACE_EAC2PP       X       X       X         FIA_UAU.6/CACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/CACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC1PP       -       -       -      <		-	-	-
FCS_COP.1/SSCDPP       -       -       X         FIA_AFL.1/Suspend_PIN_EAC2PP       X       X       X         FIA_AFL.1/Block_PIN_EAC2PP       X       X       X         FIA_API.1/CA_EAC2PP       X       X       X         FIA_API.1/CA_EAC2PP       X       X       X         FIA_API.1/RL_EAC2PP       -       X       X         FIA_UID.1/PACE_EAC2PP       X       X       X         FIA_UID.1/PACE_EAC2PP       X       X       X         FIA_UID.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -	————————	-	-	- V
FIA_AFL.1/Suspend_PIN_EAC2PP         X         X         X           FIA_AFL.1/Block_PIN_EAC2PP         X         X         X           FIA_API.1/CA_EAC2PP         X         X         X           FIA_API.1/R_EAC2PP         -         X         X           FIA_UID.1/PACE_EAC2PP         -         X         X           FIA_UID.1/PACE_EAC2PP         X         X         X           FIA_UID.1/PACE_EAC2PP         X         X         X           FIA_UAU.1/PACE_EAC2PP         X         X         X           FIA_UAU.1/PACE_EAC2PP         X         X         X           FIA_UAU.1/PACE_EAC2PP         X         X         X           FIA_UAU.4/PACE_EAC2PP         X         X         X           FIA_UAU.5/PACE_EAC2PP         X         X         X           FIA_UAU.6/CA_EAC2PP         X         X         X           FIA_UAU.6/CA_EAC2PP         X         X         X           FIA_UAU.6/PACE_EAC1PP         -         -         -           FIA_UAU.1/PACE_EAC1PP         -         -         -           FIA_UAU.4/PACE_EAC1PP         -         -         -           FIA_UAU.5/PACE_EAC1PP         -         -		-	-	
FIA_AFL.1/Block_PIN_EAC2PP       X       X       X         FIA_API.1/CA_EAC2PP       X       X       X         FIA_API.1/RI_EAC2PP       -       X       -         FIA_UID.1/PACE_EAC2PP       -       X       X         FIA_UID.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.5/PACE_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC1PP       -       -       -		- V	-	
FIA_API.1/CA_EAC2PP         X         X         X         X           FIA_API.1/RI_EAC2PP         -         X         -           FIA_UID.1/PACE_EAC2PP         X         X         X           FIA_UID.1/PACE_EAC2PP         X         X         X           FIA_UAU.1/PACE_EAC2PP         X         X         X           FIA_UAU.1/PACE_EAC2PP         X         X         X           FIA_UAU.1/PACE_EAC2PP         X         X         X           FIA_UAU.4/PACE_EAC2PP         X         X         X           FIA_UAU.5/PACE_EAC2PP         X         X         X           FIA_UAU.6/CA_EAC2PP         X         X         X           FIA_UAU.6/CA_EAC2PP         X         X         X           FIA_UAU.6/CA_EAC2PP         X         X         X           FIA_UAU.6/PACE_EAC2PP         X         X         X           FIA_UAU.6/PACE_EAC2PP         X         X         X           FIA_UAU.6/PACE_EAC1PP         -         -         -           FIA_UAU.6/PACE_EAC1PP         -         -         -           FIA_UAU.6/PACE_EAC1PP         -         -         -           FIA_UAU.6/PACE_EAC1PP         -         -				
FIA_API.1/RI_EAC2PP       -       X       -         FIA_UID.1/PACE_EAC2PP       X       X       X         FIA_UID.1/EAC2_Terminal_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/EAC2_Terminal_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.5/PACE_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.1/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -				
FIA_UID.1/PACE_EAC2PP         X         X         X           FIA_UID.1/EAC2_Terminal_EAC2PP         X         X         X           FIA_UAU.1/PACE_EAC2PP         X         X         X           FIA_UAU.1/PACE_EAC2PP         X         X         X           FIA_UAU.1/EAC2_Terminal_EAC2PP         X         X         X           FIA_UAU.4/PACE_EAC2PP         X         X         X           FIA_UAU.5/PACE_EAC2PP         X         X         X           FIA_UAU.6/CA_EAC2PP         X         X         X           FIA_UAU.6/CA_EAC2PP         X         X         X           FIA_UAU.6/CA_EAC2PP         X         X         X           FIA_UAU.6/PACE_EAC2PP         X         X         X           FIA_UAU.6/PACE_EAC2PP         X         X         X           FIA_UAU.6/PACE_EAC1PP         -         -         -           FIA_UAU.1/PACE_EAC1PP         -         -         -           FIA_UAU.5/PACE_EAC1PP         -         -         -           FIA_UAU.6/PACE_EAC1PP         -         -         -           FIA_UAU.6/PACE_EAC1PP         -         -         -           FIA_UAU.6/PACE_EAC1PP         - <t< td=""><td></td><td>λ</td><td></td><td></td></t<>		λ		
FIA_UID.1/EAC2_Terminal_EAC2PP       X       X       X         FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/EAC2_Terminal_EAC2PP       X       X       X         FIA_UAU.1/EAC2_Terminal_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.5/PACE_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.1/PACE_EAC1PP       -       -       -         FIA_UAU.5/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/EAC_EAC1PP       -       -       -         FIA_API.1/EAC1PP       -       -       -       -         FIA_API.1/PACE_CAM       -       -       -       -         FIA_API.1/PACE_EAC1PP       -		- V		
FIA_UAU.1/PACE_EAC2PP       X       X       X         FIA_UAU.1/EAC2_Terminal_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.5/PACE_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.1/PACE_EAC1PP       -       -       -         FIA_UAU.5/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/EAC_EAC1PP       -       -       -         FIA_API.1/PACE_CAM       -       -       -         FIA_API.1/PACE_CAM       -       -       -         FIA_API.1/PACE_EAC1PP       -       -       -      <				
FIA_UAU.1/EAC2_Terminal_EAC2PP       X       X       X         FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.5/PACE_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_AFL.1/PACE_EAC2PP       X       X       X         FIA_AFL.1/PACE_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.1/PACE_EAC1PP       -       -       -         FIA_UAU.4/PACE_EAC1PP       -       -       -         FIA_UAU.5/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_API.1/EAC1PP       -       -       -         FIA_API.1/PACE_CAM       -       -       -         FIA_API.1/PACE_EAC1PP       -       -       -         FIA_API.1/PACE_EAC1PP       -       -       -         FIA_API.1/PACE_EAC1PP       -       -       -				
FIA_UAU.4/PACE_EAC2PP       X       X       X         FIA_UAU.5/PACE_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_AFL.1/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.1/PACE_EAC1PP       -       -       -         FIA_UAU.4/PACE_EAC1PP       -       -       -         FIA_UAU.5/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/EAC_EAC1PP       -       -       -         FIA_API.1/EAC1PP       -       -       -         FIA_API.1/PACE_CAM       -       -       -         FIA_AFL.1/PACE_EAC1PP       -       -       -         FIA_AFL.1/PACE_EAC1PP       -       -       -         FIA_AFL.1/PACE_EAC1PP       -       -       -				
FIA_UAU.5/PACE_EAC2PP       X       X       X         FIA_UAU.6/CA_EAC2PP       X       X       X         FIA_AFL.1/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC2PP       X       X       X         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.1/PACE_EAC1PP       -       -       -         FIA_UAU.5/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/PACE_EAC1PP       -       -       -         FIA_UAU.6/EAC_EAC1PP       -       -       -         FIA_API.1/EAC1PP       -       -       -         FIA_API.1/PACE_CAM       -       -       -         FIA_API.1/PACE_EAC1PP       -       -       -         FIA_AFL.1/PACE_EAC1PP       -       -       -         FIA_AFL.1/PACE_EAC1PP       -       -       -				
FIA_UAU.6/CA_EAC2PPXXXFIA_AFL.1/PACE_EAC2PPXXXFIA_UAU.6/PACE_EAC2PPXXXFIA_UID.1/PACE_EAC1PPFIA_UAU.4/PACE_EAC1PPFIA_UAU.5/PACE_EAC1PPFIA_UAU.5/PACE_EAC1PPFIA_UAU.6/PACE_EAC1PPFIA_UAU.6/PACE_EAC1PPFIA_UAU.6/PACE_EAC1PPFIA_UAU.6/PACE_EAC1PPFIA_API.1/EAC1PPFIA_API.1/PACE_CAMFIA_API.1/PACE_EAC1PPFIA_API.1/PACE_CAMFIA_API.1/PACE_EAC1PPFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_CAMFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_EAC1PPXFIA_AFL.1/SSCDPPX	<del>_</del>			
FIA_AFL.1/PACE_EAC2PPXXXFIA_UAU.6/PACE_EAC2PPXXXFIA_UAU.6/PACE_EAC1PPFIA_UAU.1/PACE_EAC1PPFIA_UAU.4/PACE_EAC1PPFIA_UAU.5/PACE_EAC1PPFIA_UAU.6/PACE_EAC1PPFIA_UAU.6/PACE_EAC1PPFIA_UAU.6/PACE_EAC1PPFIA_API.1/EAC1PPFIA_API.1/PACE_CAMFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_CAMFIA_AFL.1/PACE_CAMFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/SSCDPPX				
FIA_UAU.6/PACE_EAC2PPXXXFIA_UID.1/PACE_EAC1PPFIA_UAU.1/PACE_EAC1PPFIA_UAU.4/PACE_EAC1PPFIA_UAU.5/PACE_EAC1PPFIA_UAU.6/PACE_EAC1PPFIA_UAU.6/EAC_EAC1PPFIA_API.1/EAC1PPFIA_API.1/PACE_CAMFIA_API.1/PACE_EAC1PPFIA_API.1/PACE_CAMFIA_API.1/SSCDPPFIA_AFL.1/SSCDPPX				
FIA_UID.1/PACE_EAC1PPFIA_UAU.1/PACE_EAC1PPFIA_UAU.4/PACE_EAC1PPFIA_UAU.5/PACE_EAC1PPFIA_UAU.6/PACE_EAC1PPFIA_UAU.6/EAC_EAC1PPFIA_API.1/EAC1PPFIA_API.1/PACE_CAMFIA_API.1/AAFIA_AFL.1/PACE_EAC1PPFIA_API.1/SSCDPPFIA_AFL.1/SSCDPPX				
FIA_UAU.1/PACE_EAC1PPFIA_UAU.4/PACE_EAC1PPFIA_UAU.5/PACE_EAC1PPFIA_UAU.6/PACE_EAC1PPFIA_UAU.6/EAC_EAC1PPFIA_API.1/EAC1PPFIA_API.1/PACE_CAMFIA_API.1/AAFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_CAMFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/SSCDPPFIA_AFL.1/SSCDPPFIA_AFL.1/SSCDPPFIA_AFL.1/SSCDPP		X		X
FIA_UAU.4/PACE_EAC1PPFIA_UAU.5/PACE_EAC1PPFIA_UAU.6/PACE_EAC1PPFIA_UAU.6/EAC_EAC1PPFIA_API.1/EAC1PPFIA_API.1/PACE_CAMFIA_API.1/AAFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_CAMFIA_API.1/AAFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/SSCDPPXFIA_AFL.1/SSCDPPX		-		-
FIA_UAU.5/PACE_EAC1PPFIA_UAU.6/PACE_EAC1PPFIA_UAU.6/EAC_EAC1PPFIA_API.1/EAC1PPFIA_API.1/PACE_CAMFIA_API.1/AAFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/SSCDPPXFIA_AFL.1/SSCDPPX		-	-	-
FIA_UAU.6/PACE_EAC1PPFIA_UAU.6/EAC_EAC1PPFIA_API.1/EAC1PPFIA_API.1/PACE_CAMFIA_API.1/AAFIA_AFL.1/PACE_EAC1PPFIA_AFL.1/SSCDPPXFIA_AFL.1/SSCDPPX		-	-	-
FIA_UAU.6/EAC_EAC1PPFIA_API.1/EAC1PPFIA_API.1/PACE_CAMFIA_API.1/AAFIA_AFL.1/PACE_EAC1PPFIA_UID.1/SSCDPPXFIA_AFL.1/SSCDPPX		-		
FIA_API.1/EAC1PP       -       -       -         FIA_API.1/PACE_CAM       -       -       -         FIA_API.1/AA       -       -       -         FIA_AFL.1/PACE_EAC1PP       -       -       -         FIA_UID.1/SSCDPP       -       -       X         FIA_AFL.1/SSCDPP       -       -       X		-		
FIA_API.1/PACE_CAM       -       -       -         FIA_API.1/AA       -       -       -         FIA_AFL.1/PACE_EAC1PP       -       -       -         FIA_UID.1/SSCDPP       -       -       X         FIA_AFL.1/SSCDPP       -       -       X				
FIA_API.1/AA       -       -       -         FIA_AFL.1/PACE_EAC1PP       -       -       -         FIA_UID.1/SSCDPP       -       -       X         FIA_AFL.1/SSCDPP       -       -       X				
FIA_AFL.1/PACE_EAC1PP         -         -         -           FIA_UID.1/SSCDPP         -         -         X           FIA_AFL.1/SSCDPP         -         X		-	-	
FIA_UID.1/SSCDPP         -         X           FIA_AFL.1/SSCDPP         -         X		-	-	-
FIA_AFL.1/SSCDPP X		-	-	-
	— — —	-	-	
		-	-	
_	FIA_UAU.1/SSCDPP	-		X
FDP_ACC.1/TRM_EAC2PPXX				
FDP_ACF.1/TRMXX	FDP_ACF.1/TRM	Х	X	Х



FDP_RIP.1/EAC2PP	Х	Х	Х
FDP_UCT.1/TRM_EAC2PP	X	X	X
FDP_UIT.1/TRM_EAC2PP	Х	Х	Х
FDP_ACC.1/TRM_EAC1PP	-	-	-
FDP_RIP.1/EAC1PP	-	-	-
FDP_UCT.1/TRM_EAC1PP	-	-	-
FDP_UIT.1/TRM_EAC1PP	-	-	-
FDP_ACC.1/SCD/SVD_Generation_SSCD	-	-	Х
PP			
FDP_ACF.1/SCD/SVD_Generation_SSCD	-	-	Х
PP			
FDP_ACC.1/SVD_Transfer_SSCDPP	-	-	Х
FDP_ACF.1/SVD_Transfer_SSCDPP	-	-	Х
FDP_ACC.1/Signature-creation_SSCDPP	-	-	Х
FDP_ACF.1/Signature-creation_SSCDPP	-	-	Х
FDP RIP.1/SSCDPP	-	-	Х
FDP_SDI.2/Persistent_SSCDPP	-	-	Х
FDP_SDI.2/DTBS_SSCDPP	-	-	X
FTP ITC.1/PACE EAC2PP	Х	Х	X X
FTP_ITC.1/CA_EAC2PP	X	X X	X X
FTP_ITC.1/PACE_EAC1PP	<u> </u>	<u> </u>	<u> </u>
FAU SAS.1/EAC2PP	X	- X	
	^	Λ	Λ
FAU_SAS.1/EAC1PP	-	-	-
FMT_MTD.1/CVCA_INI_EAC2PP	<u>X</u>	<u>X</u>	X
FMT_MTD.1/CVCA_UPD_EAC2PP	X	X	Х
FMT_SMF.1/EAC2PP	X	X	-
FMT_SMR.1	Х	Х	Х
FMT_MTD.1/DATE_EAC2PP	Х	Х	X
FMT_MTD.1/PA_EAC2PP	Х	Х	Х
FMT_MTD.1/SK_PICC_EAC2PP	Х	Х	Х
FMT_MTD.1/KEY_READ_EAC2PP	Х	Х	-
FMT_MTD.1/Initialize_PIN_EAC2PP	Х	Х	-
FMT_MTD.1/Change_PIN_EAC2PP	Х	Х	
FMT_MTD.1/Resume_PIN_EAC2PP	Х	Х	
FMT_MTD.1/Unblock_PIN_EAC2PP	Х	Х	
FMT_MTD.1/Activate_PIN_EAC2PP	Х	Х	
FMT_MTD.3/EAC2PP	Х	Х	
FMT_SMR.1/SSCDPP	-	-	Х
FMT SMF.1/SSCDPP	-	-	Х
FMT_MOF.1/SSCDPP	-	-	X
FMT_MSA.1/Admin_SSCDPP	-	-	X
FMT_MSA.1/SignatorySSCDPP			X
FMT_MSA.2/SSCDPP	-		X X
FMT_MSA.3/SSCDPP	_		X
FMT_MSA.3/SSCDPP	-	-	× X
	-	-	<u> </u>
FMT_MTD.1/Admin_SSCDPP	-	-	X X
FMT_MTD.1/Signatory_SSCDPP	-	- V	
FMT_LIM.1/EAC2PP	X X	X X	X X
FMT_LIM.2/EAC2PP	<u>X</u>	X	<u>X</u>
FMT_MTD.1/INI_ENA_EAC2PP	X	<u>X</u>	X
FMT_MTD.1/INI_DIS_EAC2PP	Х	Х	Х
FMT_SMF.1/EAC1PP	-	-	-
FMT_LIM.1/EAC1PP	-	-	-
FMT_LIM.2/EAC1PP	-	-	-



FMT_MTD.1/INI_ENA_EAC1PP	-		-
FMT_MTD.1/INI_DIS_EAC1PP	-	-	-
FMT_MTD.1/CVCA_INI_EAC1PP	-	-	-
FMT_MTD.1/CVCA_UPD_EAC1PP	-	-	-
FMT_MTD.1/DATE_EAC1PP	-	-	-
FMT_MTD.1/CAPK_EAC1PP	-	-	-
FMT_MTD.1/PA_EAC1PP	-	-	-
FMT_MTD.1/KEY_READ_EAC1PP	-	-	-
FMT_MTD.3/EAC1PP	-	-	-
FMT_LIM.1/Loader	-	Х	Х
FMT_LIM.2/Loader	-	Х	Х
FMT_MTD.1/AA_Private_Key	-	-	-
FPT_EMS.1/EAC2PP	Х	Х	Х
FPT_FLS.1/EAC2PP	Х	Х	Х
FPT_TST.1/EAC2PP	Х	Х	Х
FPT_PHP.3/EAC2PP	Х	Х	Х
FPT_TST.1/EAC1PP	-	-	
FPT_FLS.1/EAC1PP	-	-	
FPT_PHP.3/EAC1PP	-	-	
FPT_EMS.1/EAC1PP	-	-	
FPT_EMS.1/SSCDPP	-	-	Х
FPT_FLS.1/SSCDPP	-	-	Х
FPT_PHP.1/SSCDPP	-	-	Х
FPT_PHP.3/SSCDPP	-	-	Х
FPT_TST.1/SSCDPP	-	-	Х

1.4.5.3. Identity Card with EU-compliant MRTD Application

- 490 Passwords
- 491 MRZ [16]
- 492 CAN [16]
- 493 PIN [17]
- 494 PUK [17]

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

- 499 Authentication Procedure
- 500 This configuration requires implementation at the following Authentication Procedure for 501 access to non-sensitive user data of the ePassport Application:
- Advanded Inspection Procedure [16]
- 503 This configuration requires implementation of the following Authentication Procedure for 504 access any further User Data stored on the TOE:
- General Authentication Procedure [17]



506	Applications
507	ePassport Application
508	eID Application
509	eSign Application
510	Protocols
511 512	<ul> <li>PACE (Generic Mapping, Integrated Mapping and Chip Authentication Mapping) [9] [16] and [17]</li> </ul>
513	Active Authentication [7] (optionally)
514	• EAC1 [16]
515	<ul> <li>Terminal Authentication version 1 [16]</li> </ul>
516	<ul> <li>Chip Authentication version 1 [16]</li> </ul>
517	• EAC2 [17]
518	<ul> <li>Terminal Authentication version 2 [17]</li> </ul>
519	<ul> <li>Chip Authentication version 2 [17]</li> </ul>
520	Restricted Identification [17]
521	Data Groups
522	According to [17].

- 523 Data types in Table 5 Terminals and access control in Identity Card with EU-compliant MRTD 524 Application:
- Common user data: All DG, which require only BAC/PACE protocol in ePassport;
- EAC1 protected data: All DG, which require EAC1 protocol in ePassport;
- EAC2 protected data: All DG in eID and eSign application.
- 528 The authorization level of EAC1 and EAC2 terminals are determined by the effective 529 authorization calculated by from the certificate chain.
- 530 Terminals and access control

Data	PACE	EAC1	EAC2
types	terminal	terminal	terminal
Common user data	Х	Х	Х





EAC1 protected data	-	Х	-
EAC2	-	-	Х
protected data			
data			

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

FCS_CKM.1/DH_PACE_EAC2PP FCS_COP.1/SHA_EAC2PP	-		
		Х	X
		X X	X
FCS COP.1/SIG VER EAC2PP		X	X
FCS_COP.1/PACE_ENC_EAC2PP		X X	X
FCS_COP.1/PACE_ENC_EAC2PP	-	<u> </u>	X
FCS_CKM.4/EAC2PP	-	X	X
FCS_CRM.4/EAC2PP	-	X	X
FCS_CKM.1/DH_PACE_EAC1PP	X	-	Λ
FCS_CKM.4/EAC1PP	X	-	-
FCS_COP.1/PACE_ENC_EAC1PP	X	-	
FCS_COP.1/PACE_ENC_EACTPP FCS_COP.1/PACE_MAC_EACTPP	X	-	-
		-	-
FCS_RND.1/EAC1PP	X	-	-
FCS_CKM.1/CA_EAC1PP	-	-	-
FCS_COP.1/CA_ENC_EAC1PP	- 	-	-
FCS_COP.1/SIG_VER_EAC1PP	X	-	-
FCS_COP.1/CA_MAC_EAC1PP	Х	-	-
FCS_CKM.1/CA2	-	X	Х
FCS_CKM.1/RI	-	Х	-
FCS_CKM.1/AA	X	-	-
FCS_COP.1/AA	X	-	-
FCS_CKM.1/CAM	X	-	-
FCS_COP.1/CAM	Х	-	-
FCS_CKM.1/SSCDPP	-	-	Х
FCS_COP.1/SSCDPP	-	-	Х
FIA_AFL.1/Suspend_PIN_EAC2PP	Х	Х	Х
FIA_AFL.1/Block_PIN_EAC2PP	Х	Х	Х
FIA_API.1/CA_EAC2PP	-	Х	Х
FIA_API.1/RI_EAC2PP	-	Х	-
FIA_UID.1/PACE_EAC2PP	-	Х	Х
FIA_UID.1/EAC2_Terminal_EAC2PP	-	Х	Х
FIA_UAU.1/PACE_EAC2PP	-	Х	Х
FIA_UAU.1/EAC2_Terminal_EAC2PP	-	Х	Х
FIA_UAU.4/PACE_EAC2PP	-	Х	Х
FIA_UAU.5/PACE_EAC2PP	-	Х	Х
FIA_UAU.6/CA_EAC2PP	-	Х	Х
FIA_AFL.1/PACE_EAC2PP	-	Х	Х
FIA_UAU.6/PACE_EAC2PP	-	Х	Х
FIA_UID.1/PACE_EAC1PP	Х	-	-
FIA_UAU.1/PACE_EAC1PP	Х	-	-
FIA_UAU.4/PACE_EAC1PP	Х	-	-
FIA_UAU.5/PACE_EAC1PP	Х	-	-
FIA_UAU.6/PACE_EAC1PP	X	-	-
FIA_UAU.6/EAC_EAC1PP	X	-	-



	V		
FIA_API.1/EAC1PP	<u> </u>	-	-
FIA_API.1/PACE_CAM	X	-	-
FIA_API.1/AA	Х	-	-
FIA_AFL.1/PACE_EAC1PP	Х	-	-
FIA_UID.1/SSCDPP	-	-	Х
FIA_AFL.1/SSCDPP	-	-	Х
FIA_UAU.1/SSCDPP	-	-	Х
FDP_ACC.1/TRM_EAC2PP	-	Х	Х
FDP_ACF.1/TRM	Х	Х	Х
FDP_RIP.1/EAC2PP	-	Х	Х
FDP_UCT.1/TRM_EAC2PP	-	Х	Х
FDP_UIT.1/TRM_EAC2PP	-	Х	Х
FDP_ACC.1/TRM_EAC1PP	Х	-	-
FDP_RIP.1/EAC1PP	Х	-	-
FDP_UCT.1/TRM_EAC1PP	Х	-	-
FDP_UIT.1/TRM_EAC1PP	Х	-	-
FDP_ACC.1/SCD/SVD_Generation_SSCD	-	-	Х
PP			
FDP_ACF.1/SCD/SVD_Generation_SSCD	-	-	Х
PP			
FDP_ACC.1/SVD_Transfer_SSCDPP	-	-	Х
FDP_ACF.1/SVD_Transfer_SSCDPP	-	-	Х
FDP_ACC.1/Signature-creation_SSCDPP	-	-	Х
FDP_ACF.1/Signature-creation_SSCDPP	-	-	Х
FDP_RIP.1/SSCDPP	-	-	Х
FDP_SDI.2/Persistent_SSCDPP	-	-	Х
FDP_SDI.2/DTBS_SSCDPP	-	-	Х
FTP_ITC.1/PACE_EAC2PP	-	Х	Х
FTP_ITC.1/CA_EAC2PP	-	Х	Х
FTP_ITC.1/PACE_EAC1PP	Х	-	-
FAU_SAS.1/EAC2PP	-	Х	Х
FAU_SAS.1/EAC1PP	Х	-	-
FMT_MTD.1/CVCA_INI_EAC2PP	-	Х	Х
FMT_MTD.1/CVCA_UPD_EAC2PP	-	Х	Х
FMT_SMF.1/EAC2PP	-	Х	-
FMT_SMR.1	Х	Х	Х
FMT_MTD.1/DATE_EAC2PP	-	Х	Х
FMT_MTD.1/PA_EAC2PP	-	Х	Х
FMT_MTD.1/SK_PICC_EAC2PP	-	Х	Х
FMT_MTD.1/KEY_READ_EAC2PP	-	Х	-
FMT_MTD.1/Initialize_PIN_EAC2PP	-	Х	-
FMT_MTD.1/Change_PIN_EAC2PP	-	Х	
FMT_MTD.1/Resume_PIN_EAC2PP	-	Х	
FMT_MTD.1/Unblock_PIN_EAC2PP	-	Х	
FMT_MTD.1/Activate_PIN_EAC2PP	-	Х	
FMT_MTD.3/EAC2PP	-	Х	
FMT_SMR.1/SSCDPP	-	-	Х
FMT_SMF.1/SSCDPP	-	-	Х
FMT_MOF.1/SSCDPP	-	-	X
FMT_MSA.1/Admin_SSCDPP	-	-	X
FMT_MSA.1/SignatorySSCDPP	-	-	X
FMT_MSA.2/SSCDPP	-	-	X
FMT_MSA.3/SSCDPP	-	-	X X
FMT_MSA.4/SSCDPP	-	-	X X



FMT_MTD.1/Admin_SSCDPP	-	-	Х
FMT_MTD.1/Signatory_SSCDPP	-	-	Х
FMT_LIM.1/EAC2PP	-	Х	Х
FMT_LIM.2/EAC2PP	-	Х	Х
FMT_MTD.1/INI_ENA_EAC2PP	-	Х	Х
FMT_MTD.1/INI_DIS_EAC2PP	-	Х	Х
FMT_SMF.1/EAC1PP	Х	-	-
FMT_LIM.1/EAC1PP	Х	-	-
FMT_LIM.2/EAC1PP	Х	-	-
FMT_MTD.1/INI_ENA_EAC1PP	Х		-
FMT_MTD.1/INI_DIS_EAC1PP	Х	-	-
FMT_MTD.1/CVCA_INI_EAC1PP	Х	-	-
FMT_MTD.1/CVCA_UPD_EAC1PP	Х	-	-
FMT_MTD.1/DATE_EAC1PP	Х	-	-
FMT_MTD.1/CAPK_EAC1PP	Х	-	-
FMT_MTD.1/PA_EAC1PP	Х	-	-
FMT_MTD.1/KEY_READ_EAC1PP	Х	-	-
FMT_MTD.3/EAC1PP	-	-	-
FMT_LIM.1/Loader	Х	Х	Х
FMT_LIM.2/Loader	Х	Х	Х
FMT_MTD.1/AA_Private_Key	Х	-	-
FPT_EMS.1/EAC2PP	-	Х	Х
FPT_FLS.1/EAC2PP	-	Х	Х
FPT_TST.1/EAC2PP	-	Х	Х
FPT_PHP.3/EAC2PP	-	Х	Х
FPT_TST.1/EAC1PP	Х	-	
FPT_FLS.1/EAC1PP	Х	-	
FPT_PHP.3/EAC1PP	Х	-	
FPT_EMS.1/EAC1PP	Х	-	
FPT_EMS.1/SSCDPP	-	-	Х
FPT_FLS.1/SSCDPP	-	-	Х
FPT_PHP.1/SSCDPP	-	-	Х
FPT_PHP.3/SSCDPP	-	-	Х
FPT_TST.1/SSCDPP	-	-	Х
E A STREATE STREATE (CONTRACTOR )			

533 5. Application note (from the ST author)

534 Taking into consideration the [20] specifies authentication and communication protocols that 535 have to be used for the eSign application for the TOE, all the EAC2 relevant SFR are listed to 536 the eSign application as well. These SFRs contribute to secure Signature Verification Data 537 (SVD) export, Data To Be Signed (DTBS) import, and Verification Authentication Data (VAD) 538 import functionality.

539	2. CONFORMANCE	
540	2.1.CC Conform	ance Claim
541	This ST claims confor	mance to
542 543 544 545 546 547	<ul> <li>and general m</li> <li>Common Crite functional com</li> <li>Common Crite</li> </ul>	eria for Information Technology Security Evaluation, Part 1: Introduction odel; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017, [1] eria for Information Technology Security Evaluation, Part 2: Security ponents; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017, [2] eria for Information Technology Security Evaluation, Part 3: Security nponents; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017, [3]
548	as follows	
549	Part 2 extended,	
550	Part 3 conformant.	
551	The	
552 553		hodology for Information Technology Security Evaluation, Evaluation CCMB-2017-04-004, Version 3.1, Revision 5, April 2017, [4]
554	has to be taken into a	ccount.
555	2.2.PP Claim	
556	This ST claims strict	conformance to the following protection profile:
557 558	Title:	Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP] [20]
559 560 561 562	Sponsor: CC version: Assurance Level: General Status:	Bundesamt für Sicherheit in der Informationstechnik (BSI) 3.1 (Revision 3.4) EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. Final
563	Version number:	1.01

564 Registration: BSI-CC-PP-0087



565	Keywords:	ICAO, PACE, EAC, Extended Access Control, ID-Card, electronic
566		document, smart card, TR-03110
567		
568	Since the [20] claims	s strict conformance to [5], [6] and [14], this ST also claims strict
569	conformance to	
570	Title:	Machine Readable Travel Document with "ICAO Application",
571		Extended Access Control with PACE (EAC PP) [5]
572	Sponsor:	Bundesamt für Sicherheit in der Informationstechnik
573	CC Version:	3.1 (revision 3)
574	Assurance Level:	EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
575	General Status:	Final
576	Version number:	version 1.3.2
577	Registration:	BSI-CC-PP-0056-V2-2012
578	Keywords:	ICAO, Machine Readable Travel Document, Extended Access Control,
579		PACE, Supplemental Access Control (SAC)
580		
581	Title:	Common Criteria Protection Profile Electronic Document
582		implementing Extended Access Control Version 2 defined in BSI
582 583		implementing Extended Access Control Version 2 defined in BSI TR-03110 [6]
	Editor/Sponsor:	
583	Editor/Sponsor: CC Version:	TR-03110 [6]
583 584	·	TR-03110 [6] Bundesamt für Sicherheit in der Informationstechnik (BSI)
583 584 585	CC Version:	TR-03110 [6] Bundesamt für Sicherheit in der Informationstechnik (BSI) 3.1 (Revision 4)
583 584 585 586	CC Version: Assurance Level:	TR-03110 [6] Bundesamt für Sicherheit in der Informationstechnik (BSI) 3.1 (Revision 4) EAL4 augmented ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.
583 584 585 586 587	CC Version: Assurance Level: General Status:	TR-03110 [6] Bundesamt für Sicherheit in der Informationstechnik (BSI) 3.1 (Revision 4) EAL4 augmented ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. final
583 584 585 586 587 588	CC Version: Assurance Level: General Status: Version Number:	TR-03110 [6] Bundesamt für Sicherheit in der Informationstechnik (BSI) 3.1 (Revision 4) EAL4 augmented ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. final Version 1.01
583 584 585 586 587 588 589	CC Version: Assurance Level: General Status: Version Number: Registration:	TR-03110 [6] Bundesamt für Sicherheit in der Informationstechnik (BSI) 3.1 (Revision 4) EAL4 augmented ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. final Version 1.01 BSI-CC-PP-0086
583 584 585 586 587 588 589 590	CC Version: Assurance Level: General Status: Version Number: Registration:	TR-03110 [6] Bundesamt für Sicherheit in der Informationstechnik (BSI) 3.1 (Revision 4) EAL4 augmented ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. final Version 1.01 BSI-CC-PP-0086
583 584 585 586 587 588 589 590 591	CC Version: Assurance Level: General Status: Version Number: Registration: Keywords:	TR-03110 [6] Bundesamt für Sicherheit in der Informationstechnik (BSI) 3.1 (Revision 4) EAL4 augmented ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. final Version 1.01 BSI-CC-PP-0086 EAC2, eID-Application, eID-Card, PACE
583 584 585 586 587 588 589 590 591	CC Version: Assurance Level: General Status: Version Number: Registration: Keywords:	TR-03110 [6] Bundesamt für Sicherheit in der Informationstechnik (BSI) 3.1 (Revision 4) EAL4 augmented ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. final Version 1.01 BSI-CC-PP-0086 EAC2, eID-Application, eID-Card, PACE Protection profiles for Secure signature creation device — Part 2:
583 584 585 586 587 588 589 590 591 592 593	CC Version: Assurance Level: General Status: Version Number: Registration: Keywords: <b>Title:</b>	TR-03110 [6] Bundesamt für Sicherheit in der Informationstechnik (BSI) 3.1 (Revision 4) EAL4 augmented ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. final Version 1.01 BSI-CC-PP-0086 EAC2, eID-Application, eID-Card, PACE Protection profiles for Secure signature creation device — Part 2: Device with key generation
583 584 585 586 587 588 589 590 591 592 593 593	CC Version: Assurance Level: General Status: Version Number: Registration: Keywords: <b>Title:</b> Author:	TR-03110 [6] Bundesamt für Sicherheit in der Informationstechnik (BSI) 3.1 (Revision 4) EAL4 augmented ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. final Version 1.01 BSI-CC-PP-0086 EAC2, eID-Application, eID-Card, PACE Protection profiles for Secure signature creation device — Part 2: Device with key generation CEN / CENELEC (TC224/WG17)



598 Registration: BSI-CC-PP-0059-2009-MA-01

599 Keywords: secure signature-creation device, electronic signature, digital signature

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

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

- 607 Since [5] and [6] claim strict conformance to [13], this ST implicitly also claims **strict** 608 **conformance** to
- 609Title:Machine Readable Travel Document using Standard Inspection610Procedure with PACE (PACE PP) [13]
- 611 Sponsor: Bundesamt für Sicherheit in der Informationstechnik
- 612 CC Version: 3.1 (revision 4)
- 613 Assurance Level: EAL4 augmented with ALC\_DVS.2, ATE\_DPT.2 and AVA\_VAN.5
- 614 General Status: Final
- 615 Version number: Version 1.01
- 616 Registration: BSI-CC-PP-0068-V2-2011-MA-01
- 617Keywords:ePassport, travel document, ICAO, PACE, Standard Inspection618Procedure, Supplemental Access Control (SAC)
- 619

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

#### 624 **2.3.Package Claim**

625 The current ST is conformant to the following packages:

626 Assurance package EAL4 augmented with ALC\_DVS.2, ATE\_DPT.2 and AVA\_VAN.5 as 627 defined in [3].



**2.4.Conformance Rationale** 628 This ST conforms to the PPs [20], [5], [6] and [14]. This implies for this ST: 629 630 1. The TOE type of this ST is the same as the TOE type of the claimed PPs: 631 The Target of Evaluation (TOE) is an electronic document implemented as a smart 632 card programmed according to [16] and [17], and additionally representing a 633 combination of hardware and software configured to securely create, use and manage 634 signature-creation data, for the eSign application. 635 2. The security problem definition (SPD) of this ST contains the SPD of the claimed PPs. 636 The SPD contains all threats, organizational security policies and assumptions of the 637 claimed PPs. 638 The current ST extended the OSP P.Terminal because of the optional Active 639 Authentication function of TOE. 640 3. The security objectives for the TOE in this ST include all the security objectives for the 641 TOE of the claimed PPs. This objective does not weaken the security objectives of the 642 claimed PPs. In addition, the OT.Chip\_Auth\_Proof\_PACE\_CAM security objective is defined in the 643 644 ST because of the Chip Authentication mapping and OT.Chip Auth Proof AA 645 because of the Active Authentication protocol. 646 4. The security objectives for the operational environment in this ST include all security 647 objectives for the operational environment of the claimed PPs. 648 In addition the OE.Auth Key AA and OE.Exam Electronic Document AA security 649 objectives are defined in the ST because of the Active Authentication protocol. These 650 additions were necessary because none of the original security objectives for the TOE 651 or OSPs do not concern the obligations of States or Organization in connection with 652 Active Authentication protocol. 653 5. Those SFR, which are refined in order to ensure the unified terminology usage, are not 654 detailed in the following. 655 The SFRs specified in this ST include all security functional requirements (SFRs) 656 specified in the claimed PPs. We especially point to the following three refined SFRs 657 within [20]: The SFR FIA\_UAU.1/SSCDPP is redefined from [14] by additional assignments. Note 658 659 that this does not violate strict conformance to [14]. Multiple iterations of FDP\_ACF.1 and FMT\_SMR.1 exist from imported PPs to define 660 661 the access control SFPs and security roles for (common) user data, EAC1-protected


663       roles are unified to FDP_ACF.1/TRM and FMT_SMR.1.         664       The following SFRs were iterated from FCS_CKM.1, FCS_COP.1 and FIA_API.1 to         665       the ST because of PACE-CAM:         666       . FCS_CKM.1/CAM         667       . FCS_CCP.1/CAM         668       . FIA_API.1/PACE_CAM         669       The following SFR was extended to the ST because of PACE-CAM:         670       . FPT_EMS.1/EAC1PP         671       The following SFRs were refined to the ST because of PACE-CAM:         672       . FIA_UID.1/PACE_EAC1PP         673       . FIA_UAU.5/PACE_EAC1PP         674       The following SFRs were iterated from FCS_CKM.1, FCS_COP.1, FIA_API.1 and         675       . FIA_MID.1 to the ST because of Active Authentication protocol:         676       . FCS_CKM.1/AA         677       . FCS_CCP.1/AA         678       . FIA_API.1/AA         679       . FMT_MTD.1/AA         678       . FIA_API.1/AA         679       . FMT_MTD.1/AA         678       . FIA_API.1/AA         679       . FMT_MTD.1/AA         679       . FMT_MTD.1/AA         670       . FIA_API.1/AA         671       . FIA_UAU.1/PACE_EAC1PP         682       . FIA_UAU.1/	662	user data, and EAC2-protected user data. These access control SFPs and security
665       the ST because of PACE-CAM:         666       FCS_CKM.1/CAM         667       FCS_COP.1/CAM         668       FIA_API.1/PACE_CAM         669       The following SFR was extended to the ST because of PACE-CAM:         670       FFT_EMS.1/EAC1PP         671       The following SFRs were refined to the ST because of PACE-CAM:         672       FIA_UDI.1/PACE_EAC1PP         673       FIA_UAU.5/PACE_EAC1PP         674       The following SFRs were iterated from FCS_CKM.1, FCS_COP.1, FIA_API.1 and         675       FMT_MTD.1 to the ST because of Active Authentication protocol:         676       FCS_CKM.1/AA         677       FCS_COP.1/AA         678       FIA_API.1/AA         679       FMT_MTD.1/AA_Private_Key         680       The following SFRs was extended to the ST because of Active Authentication protocol:         681       FIA_UAU.1/PACE_EAC1PP         682       FPT_EMS.1/EAC1PP         683       The following SFRs were refined to the ST because of Active Authentication protocol:         684       FIA_UAU.4/PACE_EAC1PP         685       FMT_MTD.1/KEY_READ_EAC1PP         686       The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip         687       Authentication version 2 and R	663	
666       • FCS_CKM.1/CAM         667       • FCS_COP.1/CAM         668       • FIA_API.1/PACE_CAM         669       The following SFR was extended to the ST because of PACE-CAM:         670       • FPT_EMS.1/EAC1PP         671       The following SFRs were refined to the ST because of PACE-CAM:         672       • FIA_UID.1/PACE_EAC1PP         673       • FIA_UDU.J/PACE_EAC1PP         674       The following SFRs were iterated from FCS_CKM.1, FCS_COP.1, FIA_API.1 and         675       FMT_MTD.1 to the ST because of Active Authentication protocol:         676       • FCS_COP.1/AA         677       • FCS_COP.1/AA         678       • FIA_API.1/AA         679       • FMT_MTD.1/AA_Private_Key         680       The following SFRs was extended to the ST because of Active Authentication protocol:         681       • FIA_UAU.1/PACE_EAC1PP         682       • FPT_EMS.1/EAC1PP         683       The following SFRs were refined to the ST because of Active Authentication protocol:         684       • FIA_UAU.4/PACE_EAC1PP         685       • FNT_MTD.1/KEY_READ_EAC1PP         686       The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip         687       Authentication version 2 and Restricted Identification key pair(s) generation on th	664	The following SFRs were iterated from FCS_CKM.1, FCS_COP.1 and FIA_API.1 to
667       • FCS_COP.1/CAM         668       • FIA_API.1/PACE_CAM         669       The following SFR was extended to the ST because of PACE-CAM:         670       • FPT_EMS.1/EAC1PP         671       The following SFRs were refined to the ST because of PACE-CAM:         672       • FIA_UID.1/PACE_EAC1PP         673       • FIA_UAU.5/PACE_EAC1PP         674       The following SFRs were iterated from FCS_CKM.1, FCS_COP.1, FIA_API.1 and         675       FMT_MTD.1 to the ST because of Active Authentication protocol:         676       • FCS_CCP.1/AA         677       • FCS_COP.1/AA         678       • FIA_API.1/AA         679       • FMT_MTD.1/AA_Private_Key         680       The following SFRs was extended to the ST because of Active Authentication protocol:         681       • FIA_UAU.1/PACE_EAC1PP         682       • FPT_EMS.1/EAC1PP         683       The following SFRs were refined to the ST because of Active Authentication protocol:         684       • FIA_UAU.4/PACE_EAC1PP         685       • FMT_MTD.1/KEY_READ_EAC1PP         686       The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip         687       • FIA_UAU.4/PACE_EAC1PP         688       • FMT_MTD.1/SK_PICC_EAC2PP.Furthermore, these SFRs were	665	the ST because of PACE-CAM:
668       FIA_API.1/PACE_CAM         669       The following SFR was extended to the ST because of PACE-CAM:         670       • FPT_EMS.1/EAC1PP         671       The following SFRs were refined to the ST because of PACE-CAM:         672       • FIA_UID.1/PACE_EAC1PP         673       • FIA_UAU.5/PACE_EAC1PP         674       The following SFRs were iterated from FCS_CKM.1, FCS_COP.1, FIA_API.1 and         675       FMT_MTD.1 to the ST because of Active Authentication protocol:         676       • FCS_CKM.1/AA         677       • FCS_COP.1/AA         678       • FIA_API.1/AA         679       • FMT_MTD.1/AA_Private_Key         680       The following SFRs was extended to the ST because of Active Authentication protocol:         681       • FIA_UAU.1/PACE_EAC1PP         682       • FPT_EMS.1/EAC1PP         683       The following SFRs were refined to the ST because of Active Authentication protocol:         684       • FIA_UAU.4/PACE_EAC1PP         685       • FMT_MTD.1/KEY_READ_EAC1PP         686       The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip         687       • FIM_MTD.1/KEY_READ_EAC1PP         688       • FMT_MTD.1/SK_PICC_EAC2PP.         689       • FGI_MI_MID.1/SK_PICC_EAC2PP.	666	• FCS_CKM.1/CAM
669       The following SFR was extended to the ST because of PACE-CAM:         670       • FPT_EMS.1/EAC1PP         671       The following SFRs were refined to the ST because of PACE-CAM:         672       • FIA_UID.1/PACE_EAC1PP         673       • FIA_UAU.5/PACE_EAC1PP         674       The following SFRs were iterated from FCS_CKM.1, FCS_COP.1, FIA_API.1 and         675       FMT_MTD.1 to the ST because of Active Authentication protocol:         676       • FCS_CKM.1/AA         677       • FCS_COP.1/AA         678       • FIA_API.1/AA         679       • FMT_MTD.1/AA_Private_Key         680       The following SFRs was extended to the ST because of Active Authentication protocol:         681       • FIA_UAU.1/PACE_EAC1PP         682       • FPT_EMS.1/EAC1PP         683       The following SFRs were refined to the ST because of Active Authentication protocol:         684       • FIA_UAU.4/PACE_EAC1PP         685       • FMT_MTD.1/KEY_READ_EAC1PP         686       The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip         687       • FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were         688       as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were         690       • FCS_CKM.1/RI         691	667	FCS_COP.1/CAM
670       • FPT_EMS.1/EAC1PP         671       The following SFRs were refined to the ST because of PACE-CAM:         672       • FIA_UID.1/PACE_EAC1PP         673       • FIA_UAU.5/PACE_EAC1PP         674       The following SFRs were iterated from FCS_CKM.1, FCS_COP.1, FIA_API.1 and         675       FMT_MTD.1 to the ST because of Active Authentication protocol:         676       • FCS_CKM.1/AA         677       • FCS_COP.1/AA         678       • FIA_API.1/AA         679       • FMT_MTD.1/AA_Private_Key         680       The following SFRs was extended to the ST because of Active Authentication protocol:         681       • FIA_UAU.1/PACE_EAC1PP         682       • FPT_EMS.1/EAC1PP         683       The following SFRs were refined to the ST because of Active Authentication protocol:         684       • FIA_UAU.4/PACE_EAC1PP         685       • FMT_MTD.1/KEY_READ_EAC1PP         686       The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip         687       Authentication version 2 and Restricted Identification key pair(s) generation on the TOE         688       as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were         689       refined to emphasize the purpose of the SFRs:         690       • FCS_CKM.1/RI	668	• FIA_API.1/PACE_CAM
671The following SFRs were refined to the ST because of PACE-CAM:672. FIA_UID.1/PACE_EAC1PP673. FIA_UAU.5/PACE_EAC1PP674The following SFRs were iterated from FCS_CKM.1, FCS_COP.1, FIA_API.1 and675FMT_MTD.1 to the ST because of Active Authentication protocol:676. FCS_CKM.1/AA677. FCS_COP.1/AA678. FIA_API.1/AA679. FMT_MTD.1/AA_Private_Key680The following SFRs was extended to the ST because of Active Authentication protocol:681. FIA_UAU.1/PACE_EAC1PP682. FPT_EMS.1/EAC1PP683The following SFRs were refined to the ST because of Active Authentication protocol:684. FIA_UAU.4/PACE_EAC1PP685. FMT_MTD.1/KEY_READ_EAC1PP686The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip687Authentication version 2 and Restricted Identification key pair(s) generation on the TOE688as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were690. FCS_CKM.1/CA2691. FCS_CKM.1/RI692The following SFR is refined because the electronic document manufacturer may693generate or load the private keys:694. FMT_MTD.1/SK_PICC_EAC2PP695The following SFR is slightly refined in order not to confuse Chip Authentication 1 with	669	The following SFR was extended to the ST because of PACE-CAM:
672       FIA_UID.1/PACE_EAC1PP         673       FIA_UAU.5/PACE_EAC1PP         674       The following SFRs were iterated from FCS_CKM.1, FCS_COP.1, FIA_API.1 and         675       FMT_MTD.1 to the ST because of Active Authentication protocol:         676       FCS_CKM.1/AA         677       FCS_COP.1/AA         678       FIA_API.1/AA         679       FMT_MTD.1/AA_Private_Key         680       The following SFRs was extended to the ST because of Active Authentication protocol:         681       FIA_UAU.1/PACE_EAC1PP         682       FPT_EMS.1/EAC1PP         683       The following SFRs were refined to the ST because of Active Authentication protocol:         684       FIA_UAU.4/PACE_EAC1PP         685       FMT_MTD.1/KEY_READ_EAC1PP         686       The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip         687       Authentication version 2 and Restricted Identification key pair(s) generation on the TOE         688       as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were         690       FCS_CKM.1/CA2         691       FCS_CKM.1/RI         692       The following SFR is refined because the electronic document manufacturer may         693       generate or load the private keys:         694	670	FPT_EMS.1/EAC1PP
<ul> <li>FIA_UAU.5/PACE_EAC1PP</li> <li>The following SFRs were iterated from FCS_CKM.1, FCS_COP.1, FIA_API.1 and</li> <li>FMT_MTD.1 to the ST because of Active Authentication protocol:</li> <li>FCS_CKM.1/AA</li> <li>FCS_COP.1/AA</li> <li>FIA_API.1/AA</li> <li>FIA_MPI.1/AA</li> <li>FMT_MTD.1/AA_Private_Key</li> <li>Fhot following SFRs was extended to the ST because of Active Authentication protocol:</li> <li>FIA_UAU.1/PACE_EAC1PP</li> <li>FFT_EMS.1/EAC1PP</li> <li>Fhot jetting SFRs were refined to the ST because of Active Authentication protocol:</li> <li>FIA_UAU.1/PACE_EAC1PP</li> <li>FFT_EMS.1/EAC1PP</li> <li>Fhot jetting SFRs were refined to the ST because of Active Authentication protocol:</li> <li>FIA_UAU.4/PACE_EAC1PP</li> <li>FFT_EMS.1/EAC1PP</li> <li>Fhot jetting SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip</li> <li>Fhe following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip</li> <li>Authentication version 2 and Restricted Identification key pair(s) generation on the TOE</li> <li>as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were</li> <li>refined to emphasize the purpose of the SFRs:</li> <li>FCS_CKM.1/CA2</li> <li>FCS_CKM.1/RI</li> <li>FCS_CKM.1/RI</li> <li>FCS_CKM.1/SK_PICC_EAC2PP</li> <li>FM following SFR is refined because the electronic document manufacturer may</li> <li>generate or load the private keys:</li> <li>FMT_MTD.1/SK_PICC_EAC2PP</li> <li>The following SFR is slightly refined in order not to confuse Chip Authentication 1 with</li> </ul>	671	The following SFRs were refined to the ST because of PACE-CAM:
674The following SFRs were iterated from FCS_CKM.1, FCS_COP.1, FIA_API.1 and675FMT_MTD.1 to the ST because of Active Authentication protocol:676• FCS_CKM.1/AA677• FCS_COP.1/AA678• FIA_API.1/AA679• FMT_MTD.1/AA_Private_Key680The following SFRs was extended to the ST because of Active Authentication protocol:681• FIA_UAU.1/PACE_EAC1PP682• FPT_EMS.1/EAC1PP683The following SFRs were refined to the ST because of Active Authentication protocol:684• FIA_UAU.4/PACE_EAC1PP685• FMT_MTD.1/KEY_READ_EAC1PP686The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip687Authentication version 2 and Restricted Identification key pair(s) generation on the TOE688as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were690• FCS_CKM.1/CA2691• FCS_CKM.1/RI692The following SFR is refined because the electronic document manufacturer may693generate or load the private keys:694• FMT_MTD.1/SK_PICC_EAC2PP695The following SFR is slightly refined in order not to confuse Chip Authentication 1 with	672	FIA_UID.1/PACE_EAC1PP
675FMT_MTD.1 to the ST because of Active Authentication protocol:676. FCS_CKM.1/AA677. FCS_COP.1/AA678. FIA_API.1/AA679. FMT_MTD.1/AA_Private_Key680The following SFRs was extended to the ST because of Active Authentication protocol:681. FIA_UAU.1/PACE_EAC1PP682. FPT_EMS.1/EAC1PP683The following SFRs were refined to the ST because of Active Authentication protocol:684. FIA_UAU.4/PACE_EAC1PP685. FIA_UAU.4/PACE_EAC1PP686The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip687Authentication version 2 and Restricted Identification key pair(s) generation on the TOE688as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were690. FCS_CKM.1/CA2691. FCS_CKM.1/RI692The following SFR is refined because the electronic document manufacturer may693generate or load the private keys:694. FMT_MTD.1/SK_PICC_EAC2PP695The following SFR is slightly refined in order not to confuse Chip Authentication 1 with	673	FIA_UAU.5/PACE_EAC1PP
676FCS_CKM.1/AA677FCS_COP.1/AA678FIA_API.1/AA679FMT_MTD.1/AA_Private_Key680The following SFRs was extended to the ST because of Active Authentication protocol:681FIA_UAU.1/PACE_EAC1PP682FPT_EMS.1/EAC1PP683The following SFRs were refined to the ST because of Active Authentication protocol:684FIA_UAU.4/PACE_EAC1PP685FMT_MTD.1/KEY_READ_EAC1PP686The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip687Authentication version 2 and Restricted Identification key pair(s) generation on the TOE688as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were689refined to emphasize the purpose of the SFRs:690FCS_CKM.1/CA2691FCS_CKM.1/RI692The following SFR is refined because the electronic document manufacturer may693generate or load the private keys:694FMT_MTD.1/SK_PICC_EAC2PP695The following SFR is slightly refined in order not to confuse Chip Authentication 1 with	674	The following SFRs were iterated from FCS_CKM.1, FCS_COP.1, FIA_API.1 and
677FCS_COP.1/AA678FIA_API.1/AA679FMT_MTD.1/AA_Private_Key680The following SFRs was extended to the ST because of Active Authentication protocol:681FIA_UAU.1/PACE_EAC1PP682FPT_EMS.1/EAC1PP683The following SFRs were refined to the ST because of Active Authentication protocol:684FIA_UAU.4/PACE_EAC1PP685FMT_MTD.1/KEY_READ_EAC1PP686The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip687Authentication version 2 and Restricted Identification key pair(s) generation on the TOE688as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were689refined to emphasize the purpose of the SFRs:690FCS_CKM.1/CA2691FCS_CKM.1/RI692The following SFR is refined because the electronic document manufacturer may693generate or load the private keys:694FMT_MTD.1/SK_PICC_EAC2PP695The following SFR is slightly refined in order not to confuse Chip Authentication 1 with	675	FMT_MTD.1 to the ST because of Active Authentication protocol:
<ul> <li>FIA_API.1/AA</li> <li>FMT_MTD.1/AA_Private_Key</li> <li>FMT_MTD.1/AA_Private_Key</li> <li>The following SFRs was extended to the ST because of Active Authentication protocol:</li> <li>FIA_UAU.1/PACE_EAC1PP</li> <li>FFT_EMS.1/EAC1PP</li> <li>The following SFRs were refined to the ST because of Active Authentication protocol:</li> <li>FIA_UAU.4/PACE_EAC1PP</li> <li>FIA_UAU.4/PACE_EAC1PP</li> <li>FMT_MTD.1/KEY_READ_EAC1PP</li> <li>Fhe following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip</li> <li>Authentication version 2 and Restricted Identification key pair(s) generation on the TOE</li> <li>as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were</li> <li>refined to emphasize the purpose of the SFRs:</li> <li>FCS_CKM.1/CA2</li> <li>FCS_CKM.1/RI</li> <li>FCS_CKM.1/RI</li> <li>FCS_CKM.1/SK_PICC_EAC2PP</li> <li>FMT_MTD.1/SK_PICC_EAC2PP</li> <li>FMT_MTD.1/SK_PICC_EAC2PP</li> <li>The following SFR is refined because the electronic document manufacturer may</li> <li>generate or load the private keys:</li> <li>FMT_MTD.1/SK_PICC_EAC2PP</li> <li>The following SFR is slightly refined in order not to confuse Chip Authentication 1 with</li> </ul>	676	FCS_CKM.1/AA
<ul> <li>FMT_MTD.1/AA_Private_Key</li> <li>FMT_MTD.1/AA_Private_Key</li> <li>The following SFRs was extended to the ST because of Active Authentication protocol: <ul> <li>FIA_UAU.1/PACE_EAC1PP</li> <li>FPT_EMS.1/EAC1PP</li> </ul> </li> <li>The following SFRs were refined to the ST because of Active Authentication protocol: <ul> <li>FIA_UAU.4/PACE_EAC1PP</li> <li>FIA_UAU.4/PACE_EAC1PP</li> <li>FMT_MTD.1/KEY_READ_EAC1PP</li> </ul> </li> <li>Fhe following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip</li> <li>Authentication version 2 and Restricted Identification key pair(s) generation on the TOE</li> <li>as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were</li> <li>refined to emphasize the purpose of the SFRs:</li> <li>FCS_CKM.1/CA2</li> <li>FCS_CKM.1/RI</li> <li>FCS_CKM.1/RI</li> <li>Fht following SFR is refined because the electronic document manufacturer may</li> <li>generate or load the private keys:</li> <li>FMT_MTD.1/SK_PICC_EAC2PP</li> </ul> <li>The following SFR is slightly refined in order not to confuse Chip Authentication 1 with</li>	677	FCS_COP.1/AA
680The following SFRs was extended to the ST because of Active Authentication protocol:681• FIA_UAU.1/PACE_EAC1PP682• FPT_EMS.1/EAC1PP683The following SFRs were refined to the ST because of Active Authentication protocol:684• FIA_UAU.4/PACE_EAC1PP685• FMT_MTD.1/KEY_READ_EAC1PP686The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip687Authentication version 2 and Restricted Identification key pair(s) generation on the TOE688as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were689refined to emphasize the purpose of the SFRs:690• FCS_CKM.1/CA2691• FCS_CKM.1/RI692The following SFR is refined because the electronic document manufacturer may693generate or load the private keys:694• FMT_MTD.1/SK_PICC_EAC2PP695The following SFR is slightly refined in order not to confuse Chip Authentication 1 with	678	• FIA_API.1/AA
<ul> <li>FIA_UAU.1/PACE_EAC1PP</li> <li>FPT_EMS.1/EAC1PP</li> <li>FPT_EMS.1/EAC1PP</li> <li>The following SFRs were refined to the ST because of Active Authentication protocol:</li> <li>FIA_UAU.4/PACE_EAC1PP</li> <li>FMT_MTD.1/KEY_READ_EAC1PP</li> <li>FMT following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip</li> <li>Authentication version 2 and Restricted Identification key pair(s) generation on the TOE</li> <li>as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were</li> <li>refined to emphasize the purpose of the SFRs:</li> <li>FCS_CKM.1/CA2</li> <li>FCS_CKM.1/RI</li> <li>FCS_CKM.1/RI</li> <li>The following SFR is refined because the electronic document manufacturer may</li> <li>generate or load the private keys:</li> <li>FMT_MTD.1/SK_PICC_EAC2PP</li> <li>The following SFR is slightly refined in order not to confuse Chip Authentication 1 with</li> </ul>	679	FMT_MTD.1/AA_Private_Key
<ul> <li>682</li> <li>FPT_EMS.1/EAC1PP</li> <li>683</li> <li>The following SFRs were refined to the ST because of Active Authentication protocol:</li> <li>684</li> <li>FIA_UAU.4/PACE_EAC1PP</li> <li>685</li> <li>FMT_MTD.1/KEY_READ_EAC1PP</li> <li>686</li> <li>The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip</li> <li>687</li> <li>Authentication version 2 and Restricted Identification key pair(s) generation on the TOE</li> <li>688</li> <li>as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were</li> <li>689</li> <li>refined to emphasize the purpose of the SFRs:</li> <li>690</li> <li>FCS_CKM.1/CA2</li> <li>691</li> <li>FCS_CKM.1/RI</li> <li>692</li> <li>693</li> <li>694</li> <li>FMT_MTD.1/SK_PICC_EAC2PP</li> <li>The following SFR is refined because the electronic document manufacturer may</li> <li>693</li> <li>694</li> <li>FMT_MTD.1/SK_PICC_EAC2PP</li> <li>The following SFR is slightly refined in order not to confuse Chip Authentication 1 with</li> </ul>	680	The following SFRs was extended to the ST because of Active Authentication protocol:
683The following SFRs were refined to the ST because of Active Authentication protocol:684• FIA_UAU.4/PACE_EAC1PP685• FMT_MTD.1/KEY_READ_EAC1PP686The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip687Authentication version 2 and Restricted Identification key pair(s) generation on the TOE688as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were689refined to emphasize the purpose of the SFRs:690• FCS_CKM.1/CA2691• FCS_CKM.1/RI692The following SFR is refined because the electronic document manufacturer may693generate or load the private keys:694• FMT_MTD.1/SK_PICC_EAC2PP695The following SFR is slightly refined in order not to confuse Chip Authentication 1 with	681	FIA_UAU.1/PACE_EAC1PP
<ul> <li>684</li> <li>FIA_UAU.4/PACE_EAC1PP</li> <li>685</li> <li>FMT_MTD.1/KEY_READ_EAC1PP</li> <li>686</li> <li>687 The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip</li> <li>687 Authentication version 2 and Restricted Identification key pair(s) generation on the TOE</li> <li>688 as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were</li> <li>689 refined to emphasize the purpose of the SFRs:</li> <li>690</li> <li>FCS_CKM.1/CA2</li> <li>691</li> <li>FCS_CKM.1/RI</li> <li>692 The following SFR is refined because the electronic document manufacturer may</li> <li>693 generate or load the private keys:</li> <li>694</li> <li>FMT_MTD.1/SK_PICC_EAC2PP</li> <li>695 The following SFR is slightly refined in order not to confuse Chip Authentication 1 with</li> </ul>	682	FPT_EMS.1/EAC1PP
<ul> <li>FMT_MTD.1/KEY_READ_EAC1PP</li> <li>The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip</li> <li>Authentication version 2 and Restricted Identification key pair(s) generation on the TOE</li> <li>as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were</li> <li>refined to emphasize the purpose of the SFRs:</li> <li>FCS_CKM.1/CA2</li> <li>FCS_CKM.1/RI</li> <li>The following SFR is refined because the electronic document manufacturer may</li> <li>generate or load the private keys:</li> <li>FMT_MTD.1/SK_PICC_EAC2PP</li> <li>The following SFR is slightly refined in order not to confuse Chip Authentication 1 with</li> </ul>	683	The following SFRs were refined to the ST because of Active Authentication protocol:
686The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip687Authentication version 2 and Restricted Identification key pair(s) generation on the TOE688as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were689refined to emphasize the purpose of the SFRs:690• FCS_CKM.1/CA2691• FCS_CKM.1/RI692The following SFR is refined because the electronic document manufacturer may693generate or load the private keys:694• FMT_MTD.1/SK_PICC_EAC2PP695The following SFR is slightly refined in order not to confuse Chip Authentication 1 with	684	FIA_UAU.4/PACE_EAC1PP
687Authentication version 2 and Restricted Identification key pair(s) generation on the TOE688as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were689refined to emphasize the purpose of the SFRs:690. FCS_CKM.1/CA2691. FCS_CKM.1/RI692The following SFR is refined because the electronic document manufacturer may693generate or load the private keys:694. FMT_MTD.1/SK_PICC_EAC2PP695The following SFR is slightly refined in order not to confuse Chip Authentication 1 with	685	FMT_MTD.1/KEY_READ_EAC1PP
688as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were689refined to emphasize the purpose of the SFRs:690. FCS_CKM.1/CA2691. FCS_CKM.1/RI692The following SFR is refined because the electronic document manufacturer may693generate or load the private keys:694. FMT_MTD.1/SK_PICC_EAC2PP695The following SFR is slightly refined in order not to confuse Chip Authentication 1 with	686	The following SFRs are iterated from FCS_CKM.1 because the TOE supports the Chip
<ul> <li>refined to emphasize the purpose of the SFRs:</li> <li>FCS_CKM.1/CA2</li> <li>FCS_CKM.1/RI</li> <li>FCS_CKM.1/RI</li> <li>The following SFR is refined because the electronic document manufacturer may</li> <li>generate or load the private keys:</li> <li>FMT_MTD.1/SK_PICC_EAC2PP</li> <li>The following SFR is slightly refined in order not to confuse Chip Authentication 1 with</li> </ul>	687	Authentication version 2 and Restricted Identification key pair(s) generation on the TOE
<ul> <li>690 FCS_CKM.1/CA2</li> <li>691 FCS_CKM.1/RI</li> <li>692 The following SFR is refined because the electronic document manufacturer may</li> <li>693 generate or load the private keys:</li> <li>694 FMT_MTD.1/SK_PICC_EAC2PP</li> <li>695 The following SFR is slightly refined in order not to confuse Chip Authentication 1 with</li> </ul>	688	as described in FMT_MTD.1/SK_PICC_EAC2PP. Furthermore, these SFRs were
<ul> <li>691 • FCS_CKM.1/RI</li> <li>692 The following SFR is refined because the electronic document manufacturer may</li> <li>693 generate or load the private keys:</li> <li>694 • FMT_MTD.1/SK_PICC_EAC2PP</li> <li>695 The following SFR is slightly refined in order not to confuse Chip Authentication 1 with</li> </ul>	689	refined to emphasize the purpose of the SFRs:
<ul> <li>692 The following SFR is refined because the electronic document manufacturer may</li> <li>693 generate or load the private keys:</li> <li>694 • FMT_MTD.1/SK_PICC_EAC2PP</li> <li>695 The following SFR is slightly refined in order not to confuse Chip Authentication 1 with</li> </ul>	690	FCS_CKM.1/CA2
<ul> <li>693 generate or load the private keys:</li> <li>694 • FMT_MTD.1/SK_PICC_EAC2PP</li> <li>695 The following SFR is slightly refined in order not to confuse Chip Authentication 1 with</li> </ul>	691	FCS_CKM.1/RI
<ul> <li>694 • FMT_MTD.1/SK_PICC_EAC2PP</li> <li>695 The following SFR is slightly refined in order not to confuse Chip Authentication 1 with</li> </ul>	692	The following SFR is refined because the electronic document manufacturer may
695 The following SFR is slightly refined in order not to confuse Chip Authentication 1 with	693	generate or load the private keys:
	694	FMT_MTD.1/SK_PICC_EAC2PP
696 Chip Authentication 2:		
	696	Chip Authentication 2:



# 697 • FDP\_RIP.1/EAC2PP

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

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

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

# 705 **2.5.Statement of Compatibility**

# 706 2.5.1. SECURITY FUNCTIONALITIES

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

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

Platform Security Functionality	Corresponding TOE Security Functionality	Relevant or not relevant	Remarks
SF.JCVM	TSF.Platform	Relevant	Java Card Virtual Machine
SF.CONFIG	TSF.Platform	Relevant	Configuration Management
SF.OPEN	TSF.AccessControl TSF.Authenticate TSF.Platform	F.AccessControl Relevant Card Cont F.Authenticate Managem	
SF.CRYPTO TSF.AppletParametersSi gn TSF.Authenticate TSF.CryptoKey TSF.Platform		Relevant	Cryptographic Functionality
SF.RNG	RNG TSF.CryptoKey Relevant TSF.Platform		Random Number Generator
SF.DATA_STORAG E	TSF.AccessControl TSF.AppletParametersSi gn TSF.CryptoKey TSF.Platform	Relevant	Secure Data Storage



Platform Security Functionality	Corresponding TOE Security Functionality	Relevant or not relevant	Remarks
SF.PUF	-	Relevant	User Data Protection using PUF
SF.EXT_MEM	-	Not relevant	External Memory
SF.OM	TSF.Platform	Relevant	Java Object Management
SF.MM	-	Not relevant	Memory Management
SF.PIN	TSF.AppletParametersSi gn TSF.Authenticate	Relevant	PIN Management
SF.PERS_MEM	TSF.Platform	Relevant	Persistent Memory Management
SF.SENS_RES	-	Not relevant	Sensitive Result
SF.EDC	TSF.Platform	Relevant	Error Detection Code API
SF.HW_EXC	TSF.Platform	Relevant	Hardware Exception Handling
SF.RM	-	Not relevant	Restricted Mode
SF.PID	-	Not relevant	Platform Identification
SF.SMG_NSC	TSF.Platform	Relevant	No Side-Channel
SF.ACC_SBX	-	Not relevant	Secure Box
SF.MOD_INVOC	-	Not relevant	Module Invocation
SF.MOD_INVOC	- Table 6 Classification of F		Module Invocation

712

Table 6 Classification of Platform-TSFs

- 713 All the above SFs of [23], which are indicated as relevant are relevant for this ST.
- 714 2.5.2. OSPs

P.Trustworthy\_PKI, P.Terminal, P.Sensitive\_Data, P.Personalisation, 715 P.Card PKI, P.EAC2\_Terminal, P.RestrictedIdentity and P.Terminal\_PKI are not applicable to the Platform 716 717 and therefore not mappable for [23].

718 The OSP.VERIFICATION, OSP.PROCESS-TOE, OSP.KEY-CHANGE are covered by the ALC class, furthermore P.Manufact, P.Pre-Operational and P.Lim\_Block\_Loader correspond 719 720 to these OSPs.

- 721 OSP.SECURE-BOX and OSP.SECURITY-DOMAINS do not deal with any additional security 722 components.
- 2.5.3. SECURITY OBJECTIVES 723
- 724 These objectives from [23] can be mapped to this ST's objectives as shown in the following
- 725 table, so they are relevant.

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



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



	OT.Identification
	OT.Sens_Data_Conf
	OT.Tracing
	OT.RI_EAC2
	OT.Sens_Data_EAC2
OT.COMM_INTEGRITY	OT.Lifecycle_Security
	OT.AC Pers
	OT.Chip_Auth_Proof
	OT.Chip_Auth_Proof_PACE_CAM
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Identification
	OT.Sens_Data_Conf
	OT.Tracing
	OT.Sig_Secure
	OT.TOE_QSCD_Auth
	OT.TOE_TC_SVD_Exp
	OT.RI_EAC2
	OT.Sens_Data_EAC2
OT.COMM AUTH	OT.AC Pers
_	OT.Chip_Auth_Proof
	OT.Chip_Auth_Proof_PACE_CAM
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Identification
	OT.Sens_Data_Conf
	OT.Tracing
	OT.RI_EAC2
	OT.AC_PERS_EAC2
	OT.Sens_Data_EAC2
OT.DOMAIN-RIGHTS	OT.AC_Pers
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Identification
	OT.Sens_Data_Conf
OT.GLOBAL_ARRAYS_CONFID	OT.SCD_Secrecy
	OT.Sigy_SigF
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Sens_Data_EAC2
OT.IDENTIFICATION	 OT.AC_Pers
OT.IDENTIFICATION OT.KEY-MNGT	OT.AC_Pers OT.Identification OT.Lifecycle_Security
	OT.AC_Pers OT.Identification



1	OT.SCD_Secrecy
	OT.Sig_Secure
	OT.TOE_QSCD_Auth
	OT.TOE_TC_SVD_Exp
	OT.Sigy_SigF
	OT.AC Pers
	OT.Chip_Auth_Proof
	OT.Chip_Auth_Proof_PACE_CAM
	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Integrity
	OT.Prot Inf Leak
	OT.Prot_Malfunction
	OT.Sens_Data_Conf
	OT.CA2
	OT.RI EAC2
	OT.Sens_Data_EAC2
OT.OPERATE	OT.SCD Secrecy
OT.OPERATE	OT.Data_Integrity
	OT.Prot Inf Leak
	OT.Prot Malfunction
	OT.Prot_Phys-Tamper
OT.PIN-MNGT	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Confidentiality OT.Data_Integrity
	OT.Prot_Inf_Leak
	OT.Prot Malfunction
	OT.Sens_Data_EAC2
OT.REALLOCATION	OT.Data_Authenticity
OTREALEOCATION	OT.Data_Confidentiality
	OT.Data_Confidentiality OT.Data_Integrity
	OT.Sens Data EAC2
OT.RESOURCES	OT.Data_Integrity
OT.RESOURCES	OT.Prot Inf Leak
	OT.Prot_Phys-Tamper
OT.RND	OT.AC_Pers
OT.RID	OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Confidentiality OT.Data_Integrity
	OT.Sens_Data_Conf
	OT.Sens Data EAC2
OT.RNG	OT.AC Pers
	OT.AC_Pers OT.Data_Authenticity
	OT.Data_Confidentiality
	OT.Data_Confidentiality OT.Data_Integrity
	OT.Sens_Data_Conf
	OT.Sens_Data_Con OT.Sens_Data_EAC2
OT.SCP.IC	OT.AC Pers
	OT.Data_Integrity OT.Prot Inf Leak

	OT.Prot_Phys-Tamper		
OT.SCP.RECOVERY	OT.Data_Integrity		
	OT.Prot_Inf_Leak		
	OT.Prot_Phys-Tamper		
OT.SCP.SUPPORT	OT.AC_Pers		
	OT.Chip_Auth_Proof		
	OT.Chip_Auth_Proof_PACE_CAM		
	OT.Data_Authenticity		
	OT.Data_Confidentiality		
	OT.Data_Integrity		
	OT.Sens_Data_Conf		
	OT.Tracing		
	OT.CA2		
	OT.RI_EAC2		
	OT.Sens_Data_EAC2		
OT.SID_MODULE	OT.Prot_Inf_Leak		
	OT.Prot_Malfunction		
OT.TRANSACTION	OT.Data_Authenticity		
	OT.Data_Confidentiality		
	OT.Data_Integrity		
	OT.Sens_Data_EAC2		
Table 7 Manning of security objectives for the TOF			

726

Table 7 Mapping of security objectives for the TOE

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

728 ST:

729	• OT.SID
730	OT.APPLI-AUTH
731	OT.ATTACK-COUNTER
732	• OT.EXT-MEM
733	OT.FIREWALL
734	OT.Global_ARRAYS_INTEG
735	OT.NATIVE
736	OT.OBJ-DELETION
737	OT.RESTRICTED-MODE
738	OT.SEC_BOX_FW
739	OT.SENSITIVE_RESULT_INTEG

cannot be mapped because these are out of scope.

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

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



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

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

# 743 **2.5.4.** SECURITY REQUIREMENTS

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

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
FAU_ARP.1	FPT_PHP.3/EAC2PP FPT_PHP.3/EAC1PP FPT_PHP.3/SSCDPP	RP_SFR-MECH	FAU_ARP.1 facilitate to protect the TOE as required by these SFRs./SSCD
FAU_SAS.1[SCP]	FAU_SAS.1/EAC2PP FAU_SAS.1/EAC1PP	RP_SFR-MECH	FAU_SAS.1[SCP] covers these SFRs.
FCO_NRO.2[SC]	-	IP_SFR	-
FCS_CKM.1t	-	IP_SFR	-
FCS_COP.1	FCS_CKM.1/DH_PACE_E AC2PP FCS_CKM.1/DH_PACE_E AC1PP	RP_SFR-SERV	FCS_COP.1.1[ECDHPACEKeyA greement] is applied for key agreement during the PACE and CA2 protocols. FCS_COP1.1[SHA] is applied for session key derivation during PACE, protocols.



Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
	FCS_CKM.1/CAM	RP_SFR-SERV	FCS_COP.1.1[ECDHPACEKeyA greement] is applied for key agreement during the PACE- CAM.
	FCS_CKM.1/CA2	RP_SFR-SERV	FCS_CKM.1.1 is applied for generation chip authentication key(s) pair on the TOE:
	FCS_CKM.1/RI	RP_SFR-SERV	FCS_CKM.1.1 is applied for generation chip restricted identification key pair(s) on the TOE:
	FCS_CKM.1/AA	RP_SFR-SERV	FCS_CKM.1.1 is applied for generation chip active authentication key pair on the TOE:
	FCS_CKM.1/SSCDPP	RP_SFR-SERV	FCS_CKM.1.1 is applied for generation chip SCD/SVD key pair on the TOE:
	FCS_COP.1/PACE_ENC_ EAC2PP	RP_SFR-SERV	FCS_COP1.1[AES] is applied for nonce encryption during the PACE protocol. FCS_COP1.1[AES] is applied for encryption and decryption during secure messaging (PACE)
	FCS_COP.1/PACE_ENC_ EAC1PP	RP_SFR-SERV	FCS_COP1.1[AES] or FCS_COP.1[TripleDES] is applied for nonce encryption during the PACE-CAM protocol. FCS_COP1.1[AES] or FCS_COP.1[TripleDES] is applied for encryption and decryption during secure messaging (PACE).
	FCS_COP.1/SHA_EAC2P P	RP_SFR-SERV	FCS_COP1.1[SHA] is applied for session key derivation during CA2 and ephemeral key compression (CA2 and TA2).
	FCS_COP.1/CAM	RP_SFR-SERV	FCS_COP.1.1[AES] is applied for message encryption of Chip Authentication Data.
	FCS_CKM.1/CA_EAC1PP	RP_SFR-SERV	FCS_COP.1.1[ECDHPACEKeyA greement] is applied for key agreement related to CA1 FCS_COP1.1[SHA] is applied for session key derivation during CA1.
	FCS_COP.1/SIG_VER_EA C2PP	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePK CS1] orFCS_COP.1.1[ECSignature]



Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
			for digital signature verification related to TA2.
	FCS_COP.1/PACE_MAC_ EAC2PP	RP_SFR-SERV	FCS_COP.1.1[AESMAC] is applied to generate and verify the message authentication codes.
	FCS_COP.1/PACE_MAC_ EAC1PP	RP_SFR-SERV	FCS_COP.1.1[DESMAC] or FCS_COP.1.1[AESMAC] is applied to generate and verify the message authentication codes.
	FCS_COP.1/CA_ENC_EA C1PP	RP_SFR-SERV	FCS_COP.1[TripleDES] or FCS_COP1.1[AES] is applied for encryption and decryption during secure messaging (CA1)
	FCS_COP.1/CA_MAC_E AC1PP	RP_SFR-SERV	FCS_COP.1.1[DESMAC] or FCS_COP.1.1[AESMAC] is applied to generate and verify the message authentication codes (CA1)
	FCS_COP.1/SIG_VER_EA C1PP	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePK CS1] orFCS_COP.1.1[ECSignature] for digital signature verification related to TA1.
	FCS_COP.1/AA	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePK CS1] orFCS_COP.1.1[ECSignature] for digital signature generation related to Active Authentication.
	FCS_COP.1/SSCDPP	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePK CS1] or FCS_COP.1.1[ECSignature] for digital signature creation.
	FIA_API.1/CA_EAC2PP	RP_SFR-SERV	FCS_COP.1 fAESMAC] is applied for generating the authentication token.
	FIA_API.1/RI_EAC2PP	RP_SFR-SERV	FCS_COP.1.1[ECDHPACEKeyA greement] is applied for key agreement related to RI FCS_COP1.1[SHA] is applied for restricted identification.
	FIA_UAU.5/PACE_EAC2 PP	RP_SFR-SERV	FCS_COP1.1[AESMAC] is applied during PACE secure messaging the verify the message authentication codes. FCS_COP1.1[AESMAC] is applied during CA secure messaging to verify the



Pl

message authentica codes. FCS_COP1.1[AESMA applied during secu messaging to verify message authentica codes. FCS_COP1.1[SHA] if for public key comp case DH). FIA_UAU.5/PACE_EAC1 RP_SFR-SERV FCS_COP1.1[DESMA PP FCS_COP1.1[AESMA applied during PAG	AC] is ire the ation is applied
FCS_COP1.1[AESMA applied during secu messaging to verify message authentica codes. FCS_COP1.1[SHA] i for public key comp case DH). FIA_UAU.5/PACE_EAC1 RP_SFR-SERV FCS_COP1.1[DESMA PP FCS_COP1.1[AESMA	the ation is applied
applied during secu messaging to verify message authentica codes. FCS_COP1.1[SHA] i for public key comp case DH). FIA_UAU.5/PACE_EAC1 RP_SFR-SERV FCS_COP1.1[DESMA PP FCS_COP1.1[AESMA	the ation is applied
message authentica codes. FCS_COP1.1[SHA] i for public key comp case DH). FIA_UAU.5/PACE_EAC1 RP_SFR-SERV FCS_COP1.1[DESMA PP FCS_COP1.1[AESMA	ation is applied
codes. FCS_COP1.1[SHA] i for public key comp case DH). FIA_UAU.5/PACE_EAC1 RP_SFR-SERV FCS_COP1.1[DESMA PP FCS_COP1.1[AESMA	is applied
FCS_COP1.1[SHA] i for public key comp case DH). FIA_UAU.5/PACE_EAC1 RP_SFR-SERV FCS_COP1.1[DESMA PP FCS_COP1.1[AESMA	
for public key comp         case DH).         FIA_UAU.5/PACE_EAC1       RP_SFR-SERV         FCS_COP1.1[DESMA         PP       FCS_COP1.1[AESMA	
FIA_UAU.5/PACE_EAC1       RP_SFR-SERV       FCS_COP1.1[DESMA         PP       FCS_COP1.1[AESMA	ression (in
FIA_UAU.5/PACE_EAC1RP_SFR-SERVFCS_COP1.1[DESMAPPFCS_COP1.1[AESMA	
PP FCS_COP1.1[AESMA	
	-
	-
messaging the v	
	entication
codes.	
FCS_COP1.1[DESMA	AC] or
FCS_COP1.1[AESMA	AC] is
applied during C	
messaging to ve	· ·
5	entication
codes.	A C1
FCS_COP1.1[DESMA FCS_COP1.1[AESMA	-
applied during	secure
messaging (bas	
Personalisation Age	
verify the	message
authentication code	es.
FCS_COP1.1[SHA] i	
for public key comp	ression (in
case DH).	4.01
FIA_UAU.6/PACE_EAC2 RP_SFR-SERV FCS_COP1.1[DESMA PP FCS_COP1.1[AESMA	-
PP FCS_COP1.1[AESMA FIA_UAU.6/PACE_EAC1 applied during PA	-
PP messaging the v	
	entication
codes	
FIA_UAU.6/EAC_EAC1P RP_SFR-SERV FCS_COP.1.1[AESM.	AC] o
P FCS_COP.1[DESMAG	C] is
applied for	message
authentication	code
generation and v	erification
related to PACE.	
FIA_UAU.6/CA_EAC2PP RP_SFR-SERV FCS_COP.1.1[AESM. applied for message	
authentication code	
generation and veri	
related to CA2.	
FIA_UAU.6/EAC_EAC1P RP_SFR-SERV FCS_COP.1.1[AESM	AC] o
P FCS_COP.1[DESMA(	
applied for message	
authentication code	9



Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
			generation and verification related to CA1.
	FIA_API.1/EAC1PP	RP_SFR-SERV	FCS_COP1.1[AESMAC] is applied for message authentication code verification related to CA1.
	FIA_API.1/AA	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePK CS1] or FCS_COP.1.1[ECSignature] is applied for digital signature verification for Active Authentication protocol
	FIA_API.1/PACE_CAM	RP_SFR-SERV	FCS_COP.1.1[AESMAC] is applied for chip authentication data generation related to PACE- CAM.
	FDP_UCT.1/TRM_EAC1P P	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePK CS1] or FCS_COP.1.1[ECSignature] is applied for digital signature verification for TA.
	FDP_UIT.1/TRM_EAC1P P	RP_SFR-SERV	FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during PACE secure messaging the verify the message authentication codes. FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during CA secure messaging to verify the message authentication codes. FCS_COP1.1[DESMAC] or FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during secure messaging (based on Personalisation Agent Key) to verify the message authentication codes. FCS_COP1.1[SHA] is applied for public key compression (in case DH).
	FTP_ITC.1/PACE_EAC2P P	RP_SFR-SERV	FCS_COP.1[AES] and or FCS_COP.1[AESMAC] are applied during secure messaging to protect against disclosure and modification
	FTP_ITC.1/CA_EAC2PP	RP_SFR-SERV	FCS_COP.1[AES] and FCS_COP.1[AESMAC] are applied during secure



Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
			messaging to protect against disclosure and modification
	FTP_ITC.1/PACE_EAC1P P	RP_SFR-SERV	FCS_COP.1[TripleDES]orFCS_COP.1[AES]andFCS_COP.1[DESMAC]orFCS_COP.1[AESMAC]are
			applied during secure messaging to protect against disclosure and modification
	FMT_MTD.3/EAC2PP FMT_MTD.3/EAC1PP	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePK CS1] or FCS_COP.1.1[ECSignature] is applied for digital signature verification for TA1 and TA2.
FCS_RNG.1	FCS_RND.1/EAC2PP	RP_SFR-SERV	FCS_RNG.1 provides nonce and challenge generation for PACE and TA2.
	FCS_RND.1/EAC1PP	RP_SFR-SERV	FCS_COP.1[TripleDES] or FCS_COP.1[AES] is applied during secure messaging to protect the confidentiality of transmitted and received user data.
	FIA_UAU.4/PACE_EAC2 PP	RP_SFR-SERV	FCS_RNG.1 is applied to generate fresh nonce for PACE and TA2
	FIA_UAU.4/PACE_EAC1 PP	RP_SFR-SERV	FCS_RNG.1 is applied to generate fresh nonce for PACE, TA1 and Active Authentication.
	FDP_UCT.1/TRM_EAC2P P	RP_SFR-SERV	FCS_COP.1[AESMAC] is applied during secure messaging to protect the integrity of transmitted and received user data.
	FDP_UIT.1/TRM_EAC2P P	RP_SFR-SERV	FCS_COP.1[AES] is applied during secure messaging to protect the confidentiality of transmitted and received user data.
FCS_CKM.4	FCS_CKM.4/EAC2PP	RP_SFR-SERV	FCS_CKM.4 of the Platform matches this SFR
FCS_RNG.1[HDT ]	-	IP_SFR	-
FDP_ACC.2[FIRE WALL]	-	IP_SFR	
FDP_ACF.1[FIRE WALL]	-	IP_SFR	
FDP_ACC.1[SD]	-	IP_SFR	-
FDP_ACF.1[SD]	-	IP_SFR	
FDP_ACC.2[ADE L]	-	IP_SFR	-



Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
FDP_ACF.1[ADE L]	-	IP_SFR	
FDP_ACC.2[RM]	-	IP_SFR	-
FDP_ACC.1[EXT- MEM]	-	IP_SFR	
FDP_ACF.1[EXT- MEM]	-	IP_SFR	-
FDP_ACC.2[Secu reBox]	-	IP_SFR	
FDP_ACF.1[Secu reBox]	-	IP_SFR	
FDP_ACF.1[RM]	-	IP_SFR	-
FDP_IFC.1[JCVM ]	-	IP_SFR	-
FDP_IFC.2[SC]	-	IP_SFR	-
FDP_IFC.2[CFG]	FMT_LIM.1/Loader FMT_LIM.2/Loader FMT_LIM.1/EAC2PP FMT_LIM.2/EAC2PP FMT_LIM.1/EAC1PP FMT_LIM.2/EAC1PP	RP_SFR-MECH	FDP_IFC.2[CFG] applied to protect the TOE in operational phase.
FDP_IFC.1[MOD ULAR-DESIGN]	-	IP_SFR	
FDP_IFF.1[JCVM ]	-	IP_SFR	-
FDP_IFF.1[SC]	FMT_MTD.1/INI_ENA_E AC2PP FMT_MTD.1/INI_DIS_E AC2PP FMT_MTD.1/INI_ENA_E A1PP FMT_MTD.1/INI_DIS_E AC1PP	RP_SFR-MECH	FDP_IFF.1[SC] applied to control the writing of initialization and pre- personalization data as required by these SFRs.
FDP_IFF.1[CFG]	-	IP_SFR	-
FDP_IFF.1[MOD ULAR-DESIGN]	-	IP_SFR	-
FDP_ITC.2[CCM]	-	IP_SFR	-
FDP_RIP.1[OBJE CTS]	-	IP_SFR	-
FDP_RIP.1[ABO RT]	-	IP_SFR	-
FDP_RIP.1[APD U]	-	IP_SFR	-
FDP_RIP.1[bArra y]	-	IP_SFR	-
FDP_RIP.1[Glob alArray_Refined ]	-	IP_SFR	-
FDP_RIP.1[KEYS]	FDP_RIP.1/EAC2PP FDP_RIP.1/EAC1PP FDP_RIP.1/SSCDPP	RP_SFR-MECH	FDP_RIP.1[KEYS] is applied to destroy the secure message session keys, the PACE



Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
			ephemeral private key and SCD.
FDP_RIP.1[TRAN SIENT]	-	IP_SFR	-
FDP_RIP.1[ADEL	-	IP_SFR	-
FDP_RIP.1[ODEL	-	IP_SFR	-
FDP_ROL.1[FIRE WALL]	-	IP_SFR	-
FDP_ROL.1[CCM ]	-	IP_SFR	-
FDP_SDI.2[DATA ]	FPT_TST.1/EAC2PP FPT_TST.1/EAC1PP FPT_TST.1/SSCDPP	RP_SFR-MECH	FDP_SDI.2[DATA] checks the integrity of TSF data.
	FDP_SDI.2/DTBS_SSCDP P	RP_SFR-MECH	FDP_SDI.2[DATA] is applied to protect DTBS against integrity errors.
	FDP_SDI.2/Persistent_S SCDPP	RP_SFR-MECH	FDP_SDI.2[DATA] is applied to protect SCD against integrity errors.
FDP_SDI.2[SENS ITIVE_RESULT]	-	IP_SFR	-
FDP_UIT.1[CCM]	-	IP_SFR	-
FIA_AFL.1[PIN]	FIA_AFL.1/PACE_EAC2P P	IP_SFR	FIA_AFL.1[PIN] is applied for PIN management.
	FIA_AFL.1/SSCDPP	IP_SFR	FIA_AFL.1[PIN] is applied for PIN management.
FIA_ATD.1[AID]	-	IP_SFR	-
FIA_ATD.1[MOD	-	IP_SFR	-
ULAR-DESIGN]			
FIA_UID.1[SC]	FIA_UID.1/PACE_EAC2P P FIA_UID.1/EAC2_Termin al_EAC2PP FIA_UID.1/PACE_EAC1P P	RP_SFR-MECH	FIA_UID.1[SC] handled the identifier data of the TOE.
FIA_UID.1[CFG]	-	IP_SFR	-
FIA_UID.1[RM]	-	IP_SFR	-
FIA_UID.2[AID]	-	IP_SFR	-
FIA_UID.1[MOD ULAR-DESIGN]	-	IP_SFR	
FIA_USB.1[AID]	-	IP_SFR	-
FIA_USB.1[MOD ULAR-DESIGN]	-	IP_SFR	
FIA_UAU.1[RM]	-	IP_SFR	
FIA_UAU.1[SC]	FIA_UAU.1/EAC2_Termi nal_EAC2PP FIA_UAU.1/PACE_EAC2 PP FIA_UAU.1/PACE_EAC1 PP	RP_SFR-MECH	FIA_UAU.1[SC] handled the identifier data of the TOE.

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
FIA_UAU.4[SC]	-	IP SFR	-
-	-	IP_SFR	-
E]		_	
FMT_MSA.1[JCV	-	IP_SFR	-
M]			
FMT_MSA.1[AD EL]	-	IP_SFR	-
	-	IP_SFR	-
	-	IP_SFR	-
-MEM]		_	
FMT_MSA.1[Sec	-	IP_SFR	-
ureBox]			
	-	IP_SFR	-
G]		10.050	
FMT_MSA.1[SD]	-	IP_SFR	-
	-	IP_SFR	-
]			
FMT_MSA.1[MO DULAR-DESIGN]	-	IP_SFR	-
	-	IP_SFR	-
EWALL-JCVM]		<u>"_</u> 31K	-
FMT_MSA.3[FIR	-	IP_SFR	-
EWALL]			
-	-	IP_SFR	-
M]		_	
	-	IP_SFR	-
EL]			
FMT_MSA.3[EXT	-	IP_SFR	-
-MEM]			
FMT_MSA.3[Sec ureBox]	-	IP_SFR	-
	-	IP_SFR	-
G]			
	-	IP_SFR	-
FMT_MSA.3[SC]	-	IP_SFR	-
FMT_MSA.3[RM	-	IP_SFR	-
1			
FMT_MSA.3[MO	-	IP_SFR	-
DULAR-DESIGN]			
	-	IP_SFR	-
E] FMT_MTD.3[JCR	-	IP_SFR	
E]	-		-
	-	IP_SFR	-
FMT_SMF.1[AD	-	IP_SFR	-
EL]			
FMT_SMF.1[EXT	-	IP_SFR	-
-MEM]		-	
FMT_SMF.1[Sec	-	IP_SFR	-
ureBox]			



Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
FMT_SMF.1[CFG ]	-	IP_SFR	-
FMT_SMF.1[SD]	-	IP_SFR	-
FMT_SMF.1[SC]	-	IP_SFR	-
FMT_SMF.1[RM	-	IP_SFR	-
]		_	
FMT_SMF.1[MO	-	IP_SFR	-
DULAR-DESIGN]			
FMT_SMR.1	-	IP_SFR	-
FMT_SMR.1[INS TALLER]	-	IP_SFR	-
FMT_SMR.1[AD EL]	-	IP_SFR	-
FMT_SMR.1[CF G]	-	IP_SFR	-
FMT_SMR.1[SD]	-	IP_SFR	-
FMT_SMR.1[MO DULAR-DESIGN]	-	IP_SFR	-
FPR_UNO.1	-	IP_SFR	-
FPT_EMSEC.1	FPT_EMS.1/EAC2PP FPT_EMS.1/EAC1PP FPT_EMS.1/SSCDPP	RP_SFR-MECH	FPT_EMSEC.1 of the Platform matches these SFRs.
FPT_FLS.1	FPT_FLS.1/EAC2PP	RP_SFR-MECH	FPT_FLS.1 of the Platform
	FPT_FLS.1/EAC1PP		ensures the secure state of
	FPT_FLS.1/SSCDPP		the TOE as required by FPT_FLS.1
FPT_FLS.1[INSTA LLER]	-	IP_SFR	-
FPT_FLS.1[ADEL]	-	IP_SFR	-
FPT_FLS.1[ODEL ]	-	IP_SFR	-
FPT_FLS.1[CCM]	-	IP_SFR	-
FPT_FLS.1[MOD	-	IP_SFR	-
ULAR-DESIGN]			
FPT_TDC.1	-	IP_SFR	-
FPT_RCV.3[INST ALLER]	-	IP_SFR	-
FPT_PHP.3	FPT_PHP.3/EAC2PP FPT_PHP.3/EAC1PP FPT_PHP.1/SSCDPP FPT_PHP.3/SSCDPP	RP_SFR-MECH	FPT_PHP.3 of the Platform matches these SFRs.
FTP_ITC.1[SC]	-	IP_SFR	-
ADV_SPM.1	-	IP_SFR	-

745

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

Table 8 Mapping of Security requirements



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

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

The Personalization Agent (FMT\_SMR.1) may use the GlobalPlatform function of the Platform.

757 The TOE initialization and pre-personalization (FMT\_SMF.1/EAC2PP and 758 FMT\_SMF.1/EAC1PP) rely on the Platform functions.

- 759
- 760 **2.5.5.** Assurance Requirements

This ST requires EAL 4 according to Common Criteria V3.1 R5 augmented by ALC\_DVS.2,ATE\_DPT.2 and AVA\_VAN.5.

- The [23] requires EAL 6 according to Common Criteria V3.1 R5 augmented by: ASE\_TSS.2 and ALC\_FLR.1.
- As EAL 6 covers all assurance requirements of EAL 4 all non-augmented parts of this ST will match to the [23] assurance requirements.

# 767 **2.6.Analysis**

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



- 769 **3. SECURITY PROBLEM DEFINITION**
- 770 **3.1.Introduction**
- 771 3.1.1. ASSETS
- **772** *3.1.1.1.Primary Assets*

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

# 775 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.
- 779 *Generic Security Property:* Authenticity
- This asset is equal to the one(s) of [5] and [6], which itself stem from [13].

# 781 Electronic Document Tracing Data

782 Technical information about the current and previous locations of the electronic document

783 gathered unnoticeable by the Electronic Document Holder recognizing the TOE not knowing

- any PACE password. TOE tracing data can be provided / gathered.
- 785 Generic Security Property: Unavailability

This asset is equal to the one(s) of [5] and [6], which itself stem from [13]. Note that unavailability here is required for anonymity of the Electronic Document Holder.

# 788 Sensitive User Data

- 789 User data, which have been classified as sensitive data by the electronic document issuer, e.
- g. sensitive biometric data. Sensitive user data are a subset of all user data, and are protected
- by EAC1, EAC2, or both.
- 792 Generic Security Properties: Confidentiality, Integrity, Authenticity



### 793 User Data stored on the TOE

All data, with the exception of authentication data, that are stored in the context of the application(s) on the electronic document. These data are allowed to be read out, used or modified either by a PACE terminal, or, in the case of sensitive data, by an EAC1 terminal or an EAC2 terminal with appropriate authorization level.

798 Generic Security Properties: Confidentiality, Integrity, Authenticity

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

# 802 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.

806 Generic Security Properties: Confidentiality, Integrity, Authenticity

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

812 *3.1.1.2.Secondary Assets* 

813 In order to achieve a sufficient protection of the primary assets listed above, the following 814 secondary assets also have to be protected by the TOE.

# 815 Accessibility to the TOE Functions and Data only for Authorized Subjects

- Property of the TOE to restrict access to TSF and TSF-Data stored in the TOE to authorizedsubjects only.
- 818 Generic Security Property: Availability

# 819 Genuineness of the TOE

Property of the TOE to be authentic in order to provide claimed security functionality in a properway.



#### 822 *Generic Security Property:* Availability

### 823 Electronic Document Communication Establishment Authorization Data

- 824 Restricted-revealable authorization information for a human user being used for verification of
- the authorization attempts as an authorized user (PACE password). These data are stored in
- the TOE and are not send to it.
- 827 Restricted-revealable here refers to the fact that if necessary, the Electronic Document Holder
- 828 may reveal her verification values of CAN and MRZ to an authorized person, or to a device
- 829 that acts according to respective regulations and is considered trustworthy.
- 830 *Generic Security Properties:* Confidentiality, Integrity

### 831 Secret Electronic Document Holder Authentication Data

832 Secret authentication information for the Electronic Document Holder being used for
833 verification of the authentication attempts as authorized Electronic Document Holder (PACE
834 passwords).

835 *Generic Security Properties:* Confidentiality, Integrity

#### 836 TOE internal Non-Secret Cryptographic Material

837 Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret

- 838 material used by the TOE in order to enforce its security functionality.
- 839 *Generic Security Properties:* Integrity, Authenticity

#### 840 TOE internal Secret Cryptographic Keys

- 841 Permanently or temporarily stored secret cryptographic material used by the TOE in order to
- 842 enforce its security functionality.
- 843 Generic Security Properties: Confidentiality, Integrity
- 844 7. Application note (taken from [20], application note 8)
- The above secondary assets represent TSF and TSF-Data in the sense of CC.
- 846 **3.1.2.** SUBJECTS
- 847 This ST considers the following external entities and subjects:



#### 848 Attacker

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

### 853 Country Signing Certification Authority (CSCA)

An organization enforcing the policy of the electronic document issuer, i.e. confirming correctness of user and TSF data that are stored within the electronic document. The CSCA represents the country specific root of the public key infrastructure (PKI) for the electronic document and creates Document Signer Certificates within this PKI. The CSCA also issues a self-signed CSCA certificate that has to be distributed to other countries by secure diplomatic means, see [7].

# 860 Country Verifying Certification Authority (CVCA)

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

### 866 Document Signer (DS)

An organization enforcing the policy of the CSCA. A DS signs the Document Security Object that is stored on the electronic document for Passive Authentication. A Document Signer is authorized by the national CSCA that issues Document Signer Certificate, see [7]. Note that this role is usually delegated to a Personalization Agent.

#### 871 Document Verifier (DV)

An organization issuing terminal certificates as a Certificate Authority, authorized by the corresponding CVCA to issue certificates for EAC1 terminals, EAC2 terminals respectively, see [18].

#### 875 Electronic Document Holder

A person the electronic document issuer has personalized the electronic document for.
Personalization here refers to associating a person uniquely with a specific electronic
document. This subject includes "Signatory" as defined [14].



# 879 Electronic Document Presenter

A person presenting the electronic document to a terminal and claiming the identity of the Electronic Document Holder. Note that an electronic document presenter can also be an attacker. Moreover, this subject includes "user" as defined in [14].

# 883 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.

# 889 PACE Terminal

A technical system verifying correspondence between the password stored in the electronic document and the related value presented to the terminal by the electronic document presenter. A PACE terminal implements the terminal part of the PACE protocol and authenticates itself to the electronic document using a shared password (CAN, eID-PIN, eID-PUK or MRZ). A PACE terminal is not allowed reading Sensitive User Data.

# 895 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:

- 899 (i) establishing the identity of the Electronic Document Holder for the biographic data900 in the electronic document,
- 901 (ii) enrolling the biometric reference data of the Electronic Document Holder,
- 902 (iii) writing a subset of these data on the physical electronic document (optical
  903 personalization) and storing them within the electronic document's chip (electronic
  904 personalization),
- 905 (iv) writing document meta data (i. e. document type, issuing country, expiry date, etc.)
- 906 (v) writing the initial TSF data, and
- 907 (vi) signing the Document Security Object, and the elementary files EF.CardSecurity
  908 and the EF.ChipSecurity (if applicable [7], [18]) in the role DS. Note that the role
  909 Personalization Agent may be distributed among several institutions according to



910 the operational policy of the electronic document issuer. This subject includes 911 "Administrator" as defined in [14].

# 912 EAC1 Terminal / EAC2 Terminal

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

# 918 Terminal

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

# 923 **3.2.Threats**

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the assets protected by the TOE and the method of the TOE's use in the operational environment.

# 927 T.InconsistentSec

# 928 Inconsistency of security measures

929	Adverse action:	An attacker gains read or write access to user data or TOE data
930		without being allowed to, due to an ambiguous/unintended
931		configuration of the TOE's internal access conditions of user or
932		TSF data. This may lead to a forged electronic document or
933		misuse of user data.
934	Threat agent:	having high attack potential, being in possession of one or more
934 935	Threat agent:	having high attack potential, being in possession of one or more legitimate electronic documents



#### 938 T.Interfere

### 939 Interference of security protocols

940 941	Adverse action:	An attacker uses an unintended interference of implemented security protocols to gain access to user data.
942 943	Threat agent:	having high attack potential, being in possession of one or more legitimate electronic documents
944 945	Asset:	authenticity, integrity and confidentiality of User Data stored on the TOE
946	3.2.1. THREATS FR	OM EAC1PP
947	This ST includes the follow	ing threats from [5]. They concern EAC1-protected data.
948 949	<ul><li>T.Counterfeit</li><li>T.Read_Sensitive_D</li></ul>	ata

- 950 Due to identical definitions and names they are not repeated here. For the remaining threats951 from [5], cf. Chapter 3.2.3.
- 952 **3.2.2.** THREATS FROM EAC2PP
- 953 This ST includes the following threats from the [6]. They concern EAC2-protected data.
- 954 T.Counterfeit/EAC2
- 955 T.Sensitive\_Data
- 956 Due to identical definitions and names, they are not repeated here.
- 957 **3.2.3.** THREATS FROM PACEPP
- Both [5] and [6] claim [13], and thus include the threats formulated in [13]. We list each threat
- only once here. Due to identical definitions and names, their definitions are not repeated here.

- 960 **T.Abuse-Func** • 961 **T.Eavesdropping** • 962 **T.Forgery** • 963 T.Information\_Leakage • 964 **T.Malfunction** • **T.Phys-Tamper** 965 • **T.Skimming** 966 •
- 967 T.Tracing
- 968 3.2.4. THREATS FROM SSCDPP

969 The current ST also includes all threats of [14]. These items are applicable if the eSign 970 application is operational.

- 971 T.DTBS\_Forgery
- 972 T.Hack\_Phys
- 973 T.SCD\_Derive
- 974 T.SCD\_Divulge
- 975 T.Sig\_Forgery
- 976 T.SigF\_Misuse
- 977 T.SVD\_Forgery
- 978 Due to identical definitions and names, their definitions are not repeated here.

979 **3.3.Organizational Security Policies** 

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see [1], sec. 3.2). This ST includes the OSPs from the claimed protection profiles as listed below and provides no further OSPs.

- 984 **3.3.1. OSPs FROM EAC1PP**
- 985 This ST includes the following OSPs from [5], if the TOE contains EAC1-protected data.



	IDentity Applet v3.4/eIDAS Security Target
986	P.Personalisation
987	P.Sensitive_Data
988 989	Due to identical definitions and names, they are not repeated here. For the remaining OSPs from [5], see the next sections.
990	3.3.2. OSPS FROM EAC2PP
991	This ST includes the following OSPs from [6]. They mainly concern EAC2-protected data.
992	• P.EAC2_Terminal
993	P.RestrictedIdentity
994	• P.Terminal_PKI
995 996	Due to identical definitions and names, their definitions are not repeated here. For the remaining OSPs from [6], cf. the next section.
997	3.3.3. OSPs from PACEPP
998 999 1000	This ST includes the following OSPs from [13], since both [5] and [6] claim [13]. We list each OSP only once here. Due to identical definitions and names, their definitions are not repeated here as well.
1001	• P.Card_PKI
1002	• P.Manufact
1003	• P.Pre-Operational
1004	• P.Trustworthy_PKI
1005	3.3.4. OSPS FROM SSCDPP
1006 1007	The current ST also includes all OSPs of [14]. They are applicable, if the eSign application is included.
1008	• P.CSP_QCert
1009	• P.QSign
1010	P.Sig_Non-Repud

- P.Sigy\_SSCD •
- Due to identical definitions and names, their definitions are not repeated here.

# **3.3.5.** ADDITIONAL OSPS

1014 The next OSP addresses the need of a policy for the document manufacturer. It is formulated 1015 akin to [10].

1016 P.Lim\_Block\_Loader

1017 The composite manufacturer uses the Loader for loading of Security IC Embedded Software, 1018 user data of the Composite Product or IC Dedicated Support Software in charge of the IC 1019 Manufacturer. She limits the capability and blocks the availability of the Loader in order to 1020 protect stored data from disclosure and manipulation.

1021 The ST includes the following OSP from [13], since both [5] and [6] claim [13], but the 1022 **P.Terminal** was extended because the Active Authentication protocol. The extension is 1023 marked with **bold** and the other part of the OSP remained unchanged.

# 1024 P.Terminal

- 1025 The PACE terminal shall operate their terminals as follows:
- The related terminals (PACE terminal) shall be used by terminal operators and by travel
   document holders as defined in [9].
- 1028 2. They shall implement the terminal parts of the PACE protocol [9], of the Passive 1029 Authentication [9] and use them in this order<sup>3</sup>. The PACE terminal shall use randomly and 1030 (almost) uniformly selected nonce, if required by the protocols (for generating ephemeral 1031 keys for Diffie-Hellmann).
- 1032 Furthermore the PACE terminal and EAC1 terminal shall implement the terminal parts
- 1033 of the Active Authentication protocol as described in [9].
- 1034 3. The related terminals need not to use any own credentials.

10354. They shall also store the Country Signing Public Key and the Document Signer Public Key1036(in form of  $C_{CSCA}$  and  $C_{DS}$ ) in order to enable and to perform Passive1037Authentication(determination of the authenticity of data groups stored in the travel1038document, [9]).

5. The related terminals and their environment shall ensure confidentiality and integrity of
respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI
certificates, etc.), where it is necessary for a secure operation of the TOE according to the
[13].

<sup>&</sup>lt;sup>3</sup> This order is commensurate with [9].



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

# 1047 **3.4.Assumptions**

1048 The assumptions describe the security aspects of the environment in which the TOE will be 1049 used or is intended to be used. This ST includes the assumptions from the claimed protection 1050 profiles as listed below and defines no further assumptions.

- 1051 **3.4.1.** ASSUMPTIONS FROM EAC1PP
- 1052 This ST includes the following assumptions from the [5]. They concern EAC1-protected data.
- 1053 A.Auth\_PKI
- 1054 A.Insp\_Sys

1055 Due to identical definitions and names, their definitions are not repeated here. For the 1056 remaining assumptions from [5], see the next sections.

- 1057 **3.4.2.** Assumptions from EAC2PP
- 1058 [6] only includes the assumption from [13] (see below) and defines no other assumption.
- 1059 3.4.3. ASSUMPTIONS FROM PACEPP
- 1060 This ST includes the following assumptions from [13], since both [5] and [6] claim [13].
- 1061 A.Passive\_Auth
- 1062 Due to an identical definition and name, its definition is not repeated here as well.
- 1063 **3.4.4.** Assumptions from SSCDPP
- The current ST also includes all assumptions of [14]. These items are applicable, if the eSignapplication is included.
- 1066 A.CGA
- 1067 A.SCA
- 1068 Due to identical definitions and names their definitions are not repeated here.



# 1069 **4. SECURITY OBJECTIVES**

1070 This chapter describes the security objectives for the TOE and for the TOE environment. The 1071 security objectives for the TOE environment are separated into security objectives for the 1072 development, and production environment and security objectives for the operational 1073 environment.

# **4.1.Security Objectives for the TOE**

1075 This section describes the security objectives for the TOE, addressing the aspects of identified 1076 threats to be countered by the TOE, and organizational security policies to be met by the TOE.

#### 1077 OT.Non\_Interfere

### 1078 No interference of Access Control Mechanisms

1079 The various implemented access control mechanisms must be consistent. Their 1080 implementation must not allow to circumvent an access control mechanism by exploiting an 1081 unintended implementational interference of one access control mechanism with another one.

#### 1082 OT.Chip\_Auth\_Proof\_AA

#### 1083 **Proof of the electronic documents authenticity with Active Authentication**

1084 The TOE must support the Terminal to verify the identity and authenticity of the electronic 1085 document as issued by the identified issuing State or Organisation by means of the Active 1086 Authentication protocol as defined in [7], [9]. The authenticity proof provided by electronic 1087 document shall be protected against attacks with high attack potential.

# 1088 4.1.1. SECURITY OBJECTIVES FOR THE TOE FROM EAC1PP

1089 This ST includes the following additional security objectives for the TOE from [5] that are not 1090 included in [13]. They concern EAC1-protected data.

- 1091 OT.Chip\_Auth\_Proof
- 1092 OT.Sens\_Data\_Conf

1093 Due to identical definitions and names, their definitions are not repeated here. For the 1094 remaining security objectives from [5], see the next sections.

1095 In addition, the following security objective is defined here:



#### 1096 OT.Chip\_Auth\_Proof\_PACE\_CAM

### 1097 **Proof of the electronic document's chip authenticity**

1098 The TOE must support the terminals to verify the identity and authenticity of the Electronic 1099 document's chip as issued by the identified issuing State or Organization by means of the 1100 PACE-Chip Authentication Mapping (PACE-CAM) as defined in [9]. The authenticity proof 1101 provided by electronic document's chip shall be protected against attacks with high attack 1102 potential.

1103 Application note 8 (from ST author)

1104 PACE-CAM enables much faster authentication of the of the chip than running PACE with 1105 General Mapping (according to [16]) followed by CA1. OT.Chip\_Auth\_Proof\_PACE\_CAM is 1106 intended to require the Chip to merely provide an additional means – with the same level of 1107 security – of authentication.

1108 **4.1.2.** SECURITY OBJECTIVES FOR THE TOE EAC2PP

1109 This ST includes the following additional security objectives for the TOE from [6] that are not 1110 included in [13]. They concern EAC2-protected data.

- 1111 OT.AC\_Pers\_EAC2
- 1112 **OT.CA2**
- 1113 **OT.RI\_EAC2**
- 1114 OT.Sens\_Data\_EAC2

1115 Due to identical definitions and names, their definitions are not repeated here. For the 1116 remaining security objectives from [6], see the next sections.

1117 **4.1.3.** SECURITY OBJECTIVES FOR THE TOE PACEPP

1118 Both [5] and [6] claim [13]. Therefore, the following security objectives are included as well.

1119 We list them only once here.



1120	•	OT.AC_Pers
1121	•	OT.Data_Authenticity
1122	•	OT.Data_Confidentiality
1123	•	OT.Data_Integrity
1124	•	OT.Identification
1125	•	OT.Prot_Abuse-Func
1126	•	OT.Prot_Inf_Leak
1127	•	OT.Prot_Malfunction
1128	•	OT.Prot_Phys-Tamper
1129	•	OT.Tracing

1130 Due to identical definitions and names, their definitions are not repeated here.

# 1131 **4.1.4.** SECURITY OBJECTIVES FOR THE TOE SSCDPP

1132 The current ST also includes all security objectives for the TOE of [14]. These items are 1133 applicable, if an eSign application is included.

- 1134 OT.DTBS\_Integrity\_TOE
- 1135 OT.EMSEC\_Design
- 1136 OT.Lifecycle\_Security
- 1137 OT.SCD\_Secrecy
- 1138 OT.SCD\_SVD\_Corresp
- 1139 OT.SCD\_Unique
- 1140 **OT.SCD/SVD\_Gen**
- 1141 OT.Sig\_Secure
- 1142 **OT.Sigy\_SigF**
- **1143 OT.Tamper\_ID**
- 1144 OT.Tamper\_Resistance

Due to identical definitions and names, their definitions are not repeated here as well. Note that all are formally included here, but careful analysis reveals that OT.SCD\_Secrecy, OT.DTBS\_Integrity\_TOE, OT.EMSEC\_Design, OT.Tamper\_ID, and OT.Tamper\_Resistance are actually fully or partly covered by security objectives included from [13].



# 1149 **4.1.5.** Additional Security Objectives for the TOE

1150 A loader is a part of the chip operating system that allows to load data, i.e. the file-1151 system/applet containing (sensitive) user data, TSF data etc. into the Flash memory after 1152 delivery of the smartcard to the document manufacturer.

1153 The following objective for the TOE addresses limiting the availability of the loader, and is 1154 formulated akin to [10].

# 1155 OT.Cap\_Avail\_Loader

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

1159 **4.2.Security Objectives for the Operational Environment** 

# 1160 4.2.1. SECURITY OBJECTIVES FROM EAC1PP

- This ST includes the following security objectives for the TOE from the [5]. They mainly concernEAC1-protected data.
- **OE.Auth\_Key\_Travel\_Document**
- 1164 OE.Authoriz\_Sens\_Data
- 1165 OE.Exam\_Travel\_Document
- 1166 OE.Ext\_Insp\_Systems
- 1167 OE.Prot\_Logical\_Travel\_Document

1168 Due to identical definitions and names, their definitions are not repeated here. For the 1169 remaining ones, see the next sections

# 1170 **4.2.2.** SECURITY OBJECTIVES FROM EAC2PP

1171 This ST includes the following security objectives for the TOE from the [6]. They mainly concern1172 EAC2-protected data.



1173

1174

1175

1176

1177

1178

1179

1180

1181

1182

1183

1184

1185

1186

1187

1188 1189

1190

1191

1192

1193

1194

1195

1196

1197

1198

1199

**OE.Chip\_Auth\_Key** • **OE.RestrictedIdentity** • **OE.Terminal Authentication** • Due to identical definitions and names, their definitions are not repeated here. For the remaining ones, see the next section. 4.2.3. SECURITY OBJECTIVES FROM PACEPP Both [5] and [6] claim [13]. Therefore, the following security objectives on the operational environment are included as well. We repeat them only once here. **OE.Legislative\_Compliance** • **OE.Passive\_Auth\_Sign** • • **OE.Personalisation** • **OE.Terminal** • OE.Travel\_Document\_Holder Due to identical definitions and names, they are not repeated here as well. 4.2.4. SECURITY OBJECTIVES FROM SSCDPP The current ST also includes all security objectives for the TOE of [14]. These items are applicable, if an eSign application is included. **OE.CGA\_QCert** • **OE.DTBS\_Intend** • **OE.DTBS\_Protect** • • OE.HID\_VAD • **OE.Signatory OE.SSCD\_Prov\_Service** OE.SVD\_Auth • Due to identical definitions and names, their definitions are not repeated here. 4.2.5. Additional Security Objectives for the Environment The following objective on the environment is defined akin to the objective from [10].

#### 1200 OE.Lim\_Block\_Loader

1201 The manufacturer will protect the Loader functionality against misuse, limit the capability of the 1202 Loader and terminate irreversibly the Loader after intended usage of the Loader.

**Justification:** This security objective directly addresses the threat **OT.Non\_Interfere**. This threat concerns the potential interference of different access control mechanisms, which could occur as a result of combining different applications on a smartcard. Such combination does not occur in one of the claimed PPs. Hence, this security objective for the environment does – neither mitigate a threat of one of the claimed PPs that was addressed by security objectives of that PP,– nor does it fulfill any organizational security policy of one of the claimed PPs that was meant to be addressed by security objectives of the TOE of that PP.

1210 The following objectives on the environment are introduced because of the Active 1211 Authentication

### • OE.Auth\_Key\_AA

### 1213 Electronic document Active Authentication key pair

1214 The issuing State or Organisation has to establish the necessary infrastructure in order to (i) 1215 generate the electronic document's Active Authentication Key Pair, (ii) sign (Passive 1216 Authentication) and store the Active Authentication Public Key in the Active Authentication 1217 Public Key data in EF.DG15 and (iii) support Terminals of receiving States or Organisations to 1218 verify the authenticity of the electronic document used for genuine electronic document.

1219 • OE.Exam\_Electronic\_Document\_AA

# 1220 Examination of the genuineness of the electronic document with Active Authentication

1221 The Terminal of the receiving State or Organisation perform the Active Authentication protocol 1222 according to [7] and [9] in order to verify the genuineness of the presented electronic document.

# 1223 4.3.Security Objective Rationale

Table 9 provides an overview of the security objectives' coverage. According to [1], the tracing between security objectives and the security problem definition must ensure that *1) each security objective traces to at least one threat, OSP and assumption, 2) each threat, OSP and assumption has at least one security objective tracing to it, and 3) the tracing is correct* (i.e. the main point being that security objectives for the TOE do not trace back to assumptions).



1229 This is illustrated in the following way:

1230	1.	can be inferred for security objectives from claimed PPs by looking up the security
1231		objective rationale of the claimed PPs and for newly introduced security objectives
1232		because of [20] or the newly introduced functions (i.e. OE.Lim_Block_Loader,
1233		OT.Cap_Avail_Loader, OT.Chip_Auth_Proof_AA, OE.Auth_Key_AA,
1234		OE.Exam_Electronic_Document_AA and OT.Chip_Auth_Proof_PACE_CAM) by
1235		checking the columns of Table 9,

- can be inferred for threats, OSPs and assumptions from the claimed PPs by looking up
   the security objective rationale of the claimed PPs and for newly introduced or
   extended<sup>4</sup> threats, OSPs and assumptions by checking the rows of Table 9 , and
- 1239 3. simply by checking the columns of Table 9 and the security objective rationales from1240 the claimed PPs.

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

1241

Table 9 Security Objective Rationale

- 1242 The threat **T.InconsistentSec** addresses attacks on the confidentiality and the integrity of User
- 1243 Data stored on the TOE, facilitated by the data not being protected as intended.
- 1244 OT.AC\_Pers and OT.AC\_Pers\_EAC2 define the restriction on writing or modifying data;
- 1245 OT.Data\_Authenticity, OT.Data\_Confidentiality, OT.Data\_Integrity, OT.Sens\_Data\_Conf
- 1246 (from [5]), and OT.Sens\_Data\_EAC2 require the security of stored user data as well as user
- 1247 data that are transferred between the TOE and a terminal to be secure w.r.t. authenticity,
- 1248 integrity and confidentiality.

<sup>&</sup>lt;sup>4</sup> Only the impact of the modification is marked in the table.


OT.Non\_Interfere requires the TOE's access control mechanisms to be implemented consistently and their implementations not to allow to circumvent an access control mechanism by exploiting an unintended implementational interference of one access control mechanism with another one. OT.Cap\_Avail\_Loader requires the TOE to provide limited capability of the loader functionality and irreversible termination of the loader in order to protect stored user data.

OE.Lim\_Block\_Loader requires the manufacturer to protect the loader functionality against
misuse, limit the capability of the loader, and terminate irreversibly the loader after intended
usage of the loader.

1258 The combination of these security objectives cover the threat posed by **T.InconsistentSec**.

1259 The threat **T.Interfere** addresses the attack on user data by exploiting the unintended 1260 interference of security protocols. This is directly countered by OT.Non\_Interfere, requiring the 1261 TOE's access control mechanisms to be implemented consistently, and their implementations 1262 to not allow to circumvent an access control mechanism by exploiting an unintended 1263 implementational interference of one access control mechanism with another one.

1264 The threat **T.Counterfeit** (from [5]) is countered in [5] by OT.Chip Auth Proof. That security 1265 objectives addresses the implementation of the Chip Authentication Protocol Version 1 (CA1) 1266 and thus counters the thread of counterfeiting an electronic document containing an ePassport 1267 application. Here, the additional security objective for the TOE 1268 OT.Chip\_Auth\_Proof\_PACE\_CAM is introduced. It ensures that the chip in addition to CA1 1269 also supports the PACE-Chip Authentication Mapping (PACE-CAM) protocol, which supports 1270 the same security functionality as CA1 does. PACE-CAM enables much faster authentication 1271 of the of the chip than running PACE with general mapping followed by CA1.

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

1278 The OSP **P.Lim\_Block\_Loader** addresses limiting the capability and blocking the availability 1279 of the Loader in order to protect stored data from disclosure and manipulation. This is 1280 addressed by OT.Cap\_Avail\_Loader, which requires the TOE to provide a limited capability of



the loader functionality and irreversible termination of the loader in order to protect stored user data; by OT.Non\_Interfere, which requires the TOE's access control mechanisms to be implemented consistently and their implementations not to allow to circumvent an access control mechanism by exploiting an unintended implementational interference of one access control mechanism with another one; and by OE.Lim\_Block\_Loader, which requires the manufacturer to protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.

1288 The OSP **P.Terminal** is extended to support the Active Authentication protocol. With this 1289 extension the **P.Terminal** countered by the security objective 1290 **OE.Exam\_Electronic\_Document\_AA**. The **OE.Exam\_Electronic\_Document\_AA** enforces 1291 the terminal parts of the Active Authentication.



# 1292 **5. EXTENDED COMPONTENTS DEFINITION**

1293	This ST includes all extended components from the claimed PPs. This includes	
1294	<ul> <li>FAU_SAS.1 from the family FAU_SAS from [13]</li> </ul>	
1295	<ul> <li>FCS_RND.1 from the family FCS_RND from [13]</li> </ul>	
1296	<ul> <li>FMT_LIM.1 and FMT_LIM.2 from the family FMT_LIM [13]</li> </ul>	
1297	<ul> <li>FPT_EMS.1 from the family FPT_EMS from [13]</li> </ul>	
1298	<ul> <li>FIA_API.1 from the family FIA_API from [6]</li> </ul>	
1299	9 For precise definitions we refer to [13] and [6].	



# 1300 **6. SECURITY REQUIREMENTS**

1301 This part defines detailed security requirements that shall be satisfied by the TOE. The 1302 statement of TOE security requirements shall define the *functional* and *assurance* security 1303 requirements that the TOE must satisfy in order to meet the security objectives for the TOE.

1304 Common Criteria allows several operations to be performed on security requirements on the 1305 component level: *refinement, selection, assignment and iteration*, cf. sec. 8.1 of [1]. Each of 1306 these operations is used in this ST.

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

The **selection** operation is used to select one or more options provided by CC in stating a requirement. Selections that have been made by the PP author are denoted as <u>underlined text</u>. Selections to be filled in by the ST author appear in square brackets with an indication that a selection has to be made, [selection:], and are *italicized*. Selections filled in by the ST author are denoted as <u>double underlined text</u> and a foot note where the selection choices from the PP are listed.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP author are denoted as <u>underlined text</u>. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment has to be made [assignment:], and are *italicized*. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicized <u>like this</u>. Assignments filled in by the ST author are denoted as <u>double underlined text</u>.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier. For the sake of better readability, the iteration operation may also be applied to a non-repeated single component in order to indicate that such component belongs to a certain functional cluster. In such a case, the iteration operation is applied to only one single component.



- In order to distinguish between SFRs defined here and SFRs that are taken over from PPs to
  which this ST claims strict conformance, the latter are iterated resp. renamed in the following
  way:
- 1332 /EAC1PP or /XXX\_EAC1PP [5],
- 1333 /EAC2PP or /XXX\_EAC2PP for [6],
- 1334 and /SSCDPP or /XXX\_SSCDPP for [14].
- 1335 **6.1.Security Functional Requirements**

The statements of security requirements must be internally consistent. As several different PPs
with similar SFRs are claimed, great care must be taken to ensure that these several iterated
SFRs do not lead to inconsistency.

Despite this ST claims strict conformance to [13], SFRs can be safely ignored in this ST aslong as [5] and [6] are taken into account.

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

- The SFRs apply to different data that are accessible by executing different protocols.
   Hence, they are completely separate. An example is FCS\_CKM.1/DH\_PACE from [5]
   and [6]. No remark is added in such case in the text below.
- The SFRs are equivalent. Then we list them all for the sake of completeness. Hence,
   it suffices to consider only one iteration. For such SFRs, we explicitly give a remark. An
   example is FIA\_AFL.1/PACE from [5] and [6].
- 3. The SFRs do not apply to different data or protocols, but are also not completely
  equivalent. Then these multiple SFRs are refined in such a way, that one common
  component is reached that subsumes all iterations that stem from the inclusions of the
  claimed PPs. An example is FDP\_ACF.1, which is combined here from [5] and [6].
  Such a case is also explicitly mentioned in the text.
- 1355 Thus internal consistency is not violated.



# 1356 **6.1.1. Class FCS**

1357 The following SFRs are imported due to claiming [6]. They concern cryptographic support for1358 applications that contain EAC2-protected data groups.

- 1359 FCS\_CKM.1/DH\_PACE\_EAC2PP
- 1360 FCS\_COP.1/SHA\_EAC2PP
- 1361 FCS\_COP.1/SIG\_VER\_EAC2PP
- 1362 FCS\_COP.1/PACE\_ENC\_EAC2PP
- 1363 FCS\_COP.1/PACE\_MAC\_EAC2PP
- 1364 FCS\_CKM.4/EAC2PP
- 1365 **FCS\_RND.1/EAC2PP**

#### **1366** FCS\_CKM.1/DH\_PACE\_EAC2PP

**1367** Cryptographic Key Generation – Diffie-Hellman for PACE and CA2 Session Keys

1368	Hierarchical to:	No other components
1369	Dependencies:	[FCS_CKM.2 Cryptographic key distribution or
1370		FCS_COP.1 Cryptographic operation] not fulfilled, but
1371		justified:
1372		A Diffie-Hellman key agreement is used in order to
1373		have no key distribution, therefore FCS_CKM.2 makes
1374		no sense in this case.
1375		FCS_CKM.4 Cryptographic key destruction fulfilled by
1376		FCS_CKM.4/EAC2PP

## 1377 FCS\_CKM.1.1/DH\_PACE\_EAC2PP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic
 key generation algorithm <u>Diffie-Hellman-Protocol compliant to [27] and ECDH compliant</u>
 to [26]]<sup>56</sup> and specified cryptographic key sizes <u>AES 128, 192, 256</u><sup>7</sup> that meet the following:

1381 **[17]**<sup>8</sup>

**1382 9.** Application note (taken from [6], application note 10)

<sup>&</sup>lt;sup>5</sup> [assignment: cryptographic key generation algorithm]

<sup>&</sup>lt;sup>6</sup> [selection: Diffie-Hellman-Protocol compliant to [27], ECDH compliant to [26]]

<sup>&</sup>lt;sup>7</sup> [assignment: *cryptographic key sizes*]

<sup>&</sup>lt;sup>8</sup> [assignment: *list of standards*]



1383 In the above and all subsequent related SFRs, the reference w.r.t. the PACE protocol is changed to [17], whereas [13] references [7]. The difference between the two definitions is that 1384 1385 [17] defines additional optional parameters for the command MSE:Set AT. This optional parameters (e.g. the CHAT) are technically required, since here Terminal Authentication 2 1386 (TA2) can be executed right after PACE (see FIA\_UID.1/EAC2\_Terminal\_EAC2PP). As [7] 1387 does not consider TA2, no such definition is given there. These additional parameters are 1388 optional and not used during PACE itself (only afterwards). If PACE is run without TA2 1389 afterwards. access to data on the chip is given as specified by [13]. If TA2 is run afterwards, 1390 access to data on the chip can be further restricted w.r.t. to the authorization level of the 1391 terminal. Therefore, this change of references does not violate strict conformance to [13]. We 1392 1393 treat this change of references as a refinement operation, and thus mark the changed 1394 reference using **bold** text.

- 1395 10. Application note (redefined by ST author, taken from [6], application note 11)
- 1396 Applied.
- 1397 11. Application note (taken from [6], application note 12)

1398 [13] considers Diffie-Hellman key generation only for PACE. Since the TOE is required to 1399 implement Chip Authentication 2 (cf. FIA\_API.1/CA\_EAC2PP), here 1400 FCS\_CKM.1/DH\_PACE\_EAC2PP applies for CA2 as well.

- 1401 FCS\_COP.1/SHA\_EAC2PP
- 1402 Cryptographic operation Hash for key derivation

1403	Hierarchical to:	No other components
1404	Dependencies:	[FDP_ITC.1 Import of user data without security
1405		attributes, or FDP_ITC.2 Import of user data with
1406		security attributes, or FCS_CKM.1 Cryptographic key
1407		generation] not fulfilled, but justified:
1408		A hash function does not use any cryptographic key;
1409		hence, neither a respective key import nor key
1410		generation can be expected here.
1411		FCS_CKM.4 Cryptographic key destruction not fulfilled,
1412		but <b>justified</b> :
1413		A hash function does not use any cryptographic key;
1414		hence, a respective key destruction cannot be
1415		expected here.

## 1416 FCS\_COP.1.1/SHA\_EAC2PP

- 1417 The TSF shall perform <u>hashing</u><sup>9</sup> in accordance with a specified cryptographic algorithm
- 1418 <u>SHA-1, SHA-224, SHA-256, SHA-384, SHA-512<sup>10</sup> and cryptographic key sizes none<sup>11</sup> that</u>
- 1419 meet the following:  $[28]^{12}$ .
- 1420 12. Application note (taken from [6], application note 13)

For compressing (hashing) an ephemeral public key for DH (TA2 and CA2), the hash function SHA-1 shall be used ([18]). The TOE shall implement as hash functions either SHA-1 or SHA-224 or SHA-256 for Terminal Authentication 2, cf. [18]. Within the normative Appendix of [18] 'Key Derivation Function', it is stated that the hash function SHA-1 shall be used for deriving 128-bit AES keys, whereas SHA-256 shall be used for deriving 192-bit and 256-bit AES keys.

- 1426 FCS\_COP.1/SIG\_VER\_EAC2PP
- 1427 Cryptographic operation Signature verification

1428	Hierarchical to:	No other components
1429	Dependencies:	[FDP_ITC.1 Import of user data without security
1430		attributes, or FDP_ITC.2 Import of user data with
1431		security attributes, or FCS_CKM.1 Cryptographic key
1432		generation] not fulfilled, but justified:
1433		The root key $PK_{CVCA}$ (initialization data) used for
1434		verifying the DV Certificate is stored in the TOE during
1435		its personalization in the card issuing life cycle phase <sup>13</sup> .
1436		Since importing the respective certificates (Terminal
1437		Certificate, DV Certificate) does not require any special
1438		security measures except those required by the current
1439		SFR (cf. FMT_MTD.3/EAC2PP below), the current ST
1440		does not contain any dedicated requirement like
1441		FDP_ITC.2 for the import function.
1442		FCS_CKM.4 Cryptographic key destruction not fulfilled,
1443		but <b>justified</b> :
1444		Cryptographic keys used for the purpose of the current
1445		SFR (PK <sub>PCD</sub> , PK <sub>DV</sub> , PK <sub>CVCA</sub> ) are public keys; they do
1446		not represent any secret, and hence need not to be
1447		destroyed.

<sup>&</sup>lt;sup>9</sup> [assignment: *list of cryptographic operations*]

<sup>&</sup>lt;sup>10</sup> [assignment: *cryptographic algorithm*]

<sup>&</sup>lt;sup>11</sup> [assignment: *cryptographic key sizes*]

<sup>&</sup>lt;sup>12</sup> [assignment: *list of standards*]

<sup>&</sup>lt;sup>13</sup> as already mentioned, operational use of the TOE is explicitly in focus of the ST and in the [20]



1448 FCS\_COP.1.1/SIG\_VER\_EAC2PP

1449	The TSF shall perform digital signature verification <sup>14</sup> in accordance with a specified
1450	cryptographic algorithm <u>RSA, RSA CRT and ECDSA<sup>15</sup> and cryptographic key sizes RSA:</u>
1451	<u>RSA, RSA CRT: 1024, 1280, 1536, 1984, 2048, 3072, 4096 and from 2000 bit to 4096 bit</u>
1452	<u>in one bit steps; ECDSA: 160, 192, 224, 256, 320, 384, 521 bit<sup>16</sup> that meet the following:</u>
1453	[ <u>24], [29]</u> <sup>17</sup> .
1454	13. Application note (taken from [6], application note 14)
1455	This SFR is concerned with Terminal Authentication 2, cf. [17].
1456	14. Application note (from ST author)
1457	The TOE based on the Platform functionalities supports RSA and RSA-CRT digital signature

algorithms and cryptographic key sizes 512 bits up to 4096 bits with equal security measures.
 However, to fend off attackers with high attack potential an adequate key length must be used.

1460 FCS\_COP.1/PACE\_ENC\_EAC2PP

# 1461 Cryptographic operation – Encryption/Decryption AES

1462	Hierarchical to:	No other components
1463 1464	Dependencies:	FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with
1465 1466 1467		security attributes, or FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/DH_PACE_EAC2PP
1468 1469		FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/EAC2PP

1470 FCS\_COP.1.1/PACE\_ENC\_EAC2PP

<sup>&</sup>lt;sup>14</sup> [assignment: *list of cryptographic operations*]

<sup>&</sup>lt;sup>15</sup> [assignment: *cryptographic algorithm*]

<sup>&</sup>lt;sup>16</sup> [assignment: *cryptographic key sizes*]

<sup>&</sup>lt;sup>17</sup> [assignment: *list of standards*]

# 

- 1471 The TSF shall perform <u>secure messaging encryption and decryption<sup>18</sup></u> in accordance
- 1472 with a specified cryptographic algorithm <u>AES in CBC mode<sup>19</sup></u> and cryptographic key sizes
- 1473 <u>128, 192, 256 bit<sup>20</sup> that meet the following</u>: [18]<sup>21</sup>
- 1474 15. Application note (taken from [6], application note 15)

1475 This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging 1476 with encryption of transmitted data. The related session keys are agreed between the TOE 1477 and the terminal as part of either the PACE protocol (PACE-K<sub>Enc</sub>) or Chip Authentication 2 (CA-1478 K<sub>Enc</sub>) according to FCS\_CKM.1/DH\_PACE\_EAC2PP. Note that in accordance with [18], 3DES 1479 could be used in CBC mode for secure messaging. Due to the fact that 3DES is not 1480 recommended any more (cf. [17]), 3DES in any mode is no longer applicable here.

1481 16. Application note (taken from [6], application note 16)

Refinement of FCS\_COP.1.1/PACE\_ENC\_EAC2PP, since here PACE must adhere to [18].
All references (both the one in [13] and [18]) itself reference [12] for secure messaging. [18]
however further restricts the available choice of key-sizes and algorithms. Hence, [18] is fully
(backward) compatible to the reference given in [13].

- 1486 FCS\_COP.1/PACE\_MAC\_EAC2PP
- 1487 Cryptographic operation MAC

1488	Hierarchical to:	No other components
1489 1490	Dependencies:	FDP_ITC.1 Import of user data without security
		attributes, or FDP_ITC.2 Import of user data with
1491		security attributes, or FCS_CKM.1 Cryptographic key
1492		generation] fulfilled by
1493		FCS_CKM.1/DH_PACE_EAC2PP
1494		FCS_CKM.4 Cryptographic key destruction fulfilled by
1495		FCS_CKM.4/EAC2PP

1496 FCS\_COP.1.1/PACE\_MAC\_EAC2PP

<sup>&</sup>lt;sup>18</sup> [assignment: *list of cryptographic operations*]

<sup>&</sup>lt;sup>19</sup> [selection: *cryptographic algorithm*]

<sup>&</sup>lt;sup>20</sup> [selection: 128, 192, 256 bit ]

<sup>&</sup>lt;sup>21</sup> [assignment: *list of standards*]



- 1497 The TSF shall perform <u>secure messaging message authentication code<sup>22</sup></u> in accordance
- 1498 with a specified cryptographic algorithm <u>CMAC<sup>23</sup></u> and cryptographic key sizes <u>128, 192,</u>
- 1499  $\underline{256 \text{ bit}}^{24}$  that meet the following: **[18]**<sup>25</sup>
- 1500 17. Application note (redefined by ST author, taken from [6], application note 17)
- 1501 See 16. Application note (taken from [6], application note 16).
- 1502 18. Application note (taken from [6], application note 18)

1503 This SFR removes 3DES and restricts to CMAC compared to the SFR of [13] by selection. 1504 Hence, a minimum key-size of 128 bit is required.

- 1505 FCS\_CKM.4/EAC2PP
- 1506 Cryptographic key destruction Session keys

1507	Hierarchical to:	No other components
1508	Dependencies:	FDP_ITC.1 Import of user data without security
1509		attributes, or FDP_ITC.2 Import of user data with
1510		security attributes, or FCS_CKM.1 Cryptographic key
1511		generation] fulfilled by
1512		FCS_CKM.1/DH_PACE_EAC2PP and
1513		FCS_CKM.1/CA_EAC1PP

# 1514 FCS\_CKM.4.1/EAC2PP

- 1515 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic
- 1516 key destruction method <u>physically overwriting the keys in a randomized manner<sup>26</sup> that</u>
- 1517 meets the following: <u>provided by the underlying certified Platform</u><sup>27</sup>.
- 1518 19. Application note

In [13] concerning this component requires the destruction of PACE session keys after detection of an error in a received command by verification of the MAC. While the definition of FCS\_CKM.4/EAC2PP remains unaltered, here this component also requires the destruction of sessions keys after a successful run of Chip Authentication 2. The TOE shall destroy the CA2 session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP\_RIP.1/EAC2PP.

<sup>&</sup>lt;sup>22</sup> [assignment: *list of cryptographic operations*]

<sup>&</sup>lt;sup>23</sup> [selection: *cryptographic algorithm*]

<sup>&</sup>lt;sup>24</sup> [selection: *112 128, 192, 256 bit*]

<sup>&</sup>lt;sup>25</sup> [assignment: *list of standards*]

<sup>&</sup>lt;sup>26</sup> [assignment: *cryptographic key destruction method*]

<sup>&</sup>lt;sup>27</sup> [assignment: *list of standards*]



- 1526 FCS\_RND.1/EAC2PP1527 Quality metric for random numbers
- 1528 Hierarchical to: No other components
- 1529 Dependencies: No dependencies.
- 1530 FCS\_RND.1.1/EAC2PP
- 1531 The TSF shall provide a mechanism to generate random numbers that meet <u>DRG.3<sup>28</sup></u>.
- 1532 **20.** Application note

In [13] concerning this component requires the TOE to generate random numbers (random nonce) for PACE. While the definition of FCS\_RND.1/EAC2PP remains unaltered, here this component requires the TOE to generate random numbers (random nonce) for all authentication protocols (i.e. PACE, CA2), as required by FIA\_UAU.4/PACE\_EAC2PP.

- 1537 The following SFRs are imported due to claiming [5]. They concern cryptographic support for
- applications that contain EAC1-protected data groups.
- 1539 FCS\_CKM.1/DH\_PACE\_EAC1PP
- 1540 **FCS\_CKM.4/EAC1PP**
- 1541 (equivalent to **FCS\_CKM.4/EAC2PP**, but listed here for the sake of completeness)
- 1542 FCS\_COP.1/PACE\_ENC\_EAC1PP
- 1543 FCS\_COP.1/PACE\_MAC\_EAC1PP
- 1544 21. Application note (redefined by ST author, taken from[20], application note 9)
- 1545 Applied.
- 1546 **FCS\_RND.1/EAC1PP**
- 1547 (equivalent to **FCS\_RND.1/EAC2PP**, but listed here for the sake of completeness)
- 1548 FCS\_CKM.1/CA\_EAC1PP
- 1549 FCS\_COP.1/CA\_ENC\_EAC1PP
- 1550 FCS\_COP.1/SIG\_VER\_EAC1PP
- 1551 FCS\_COP.1/CA\_MAC\_EAC1PP

<sup>&</sup>lt;sup>28</sup> [assignment: *a defined quality metric*]



1552 1553	FCS_CKM.1/DH_PACE_EAC1PP Cryptographic key generation – Diffie-	Hellman for PACE session keys
1554	Hierarchical to:	No other components
1555	Dependencies:	[FCS_CKM.2 Cryptographic key distribution or
1556		FCS_COP.1 Cryptographic operation].
1557		Justification: A Diffie-Hellman key agreement is used
1558		in order to have no key distribution, therefore
1559		FCS_CKM.2 makes no sense in this case.
1560		FCS_CKM.4 Cryptographic key destruction: fulfilled by
1561		FCS_CKM.4/EAC1PP
1562	FCS_CKM.1.1/DH_PACE_EAC1PP	
1563	The TSF shall generate cryptog	raphic keys in accordance with a specified cryptographic
1564	key generation algorithm <u>Diffie-</u>	Hellman-Protocol compliant to [27], ECDH compliant to
1565	[ <u>26]</u> <sup>2930</sup> and specified cryptograp	hic key sizes <u>TDES 128, AES 128, 192 and 256 bits</u> ³¹ that
1566	meet the following:[7] <sup>32</sup>	
1567 1568	FCS_COP.1/PACE_ENC_EAC1PP Encryption / Decryption AES / 3DES	
1569	Hierarchical to:	No other components
1570	Dependencies:	[FDP_ITC.1 Import of user data without security
1571		attributes, or FDP_ITC.2 Import of user data with
1572		security attributes, or FCS_CKM.1 Cryptographic key
1573		generation]: fulfilled by
1574		FCS_CKM.1/DH_PACE_EAC1PP.
1575		FCS_CKM.4 Cryptographic key destruction: fulfilled by
1576		FCS_CKM.4/EAC1PP.

1577 FCS\_COP.1.1/PACE\_ENC\_EAC1PP

 <sup>&</sup>lt;sup>29</sup> [assignment: cryptographic key generation algorithm]
 <sup>30</sup> [selection: Diffie-Hellman-Protocol compliant to [27], ECDH compliant to [26]]
 <sup>31</sup> [assignment: cryptographic key sizes]
 <sup>32</sup> [assignment: list of standards]



1578The TSF shall perform secure messaging – encryption and decryption33 in accordance1579with a specified cryptographic algorithm  $\underline{AES}$ ,  $\underline{3DES}^{34}$  in CBC mode35 and cryptographic1580key sizes  $\underline{3DES}$  112,  $\underline{AES}$  128, 192, 256 bit3637 that meet the following: compliant to  $[7]^{38}$ .

# 1581 FCS\_COP.1/PACE\_MAC\_EAC1PP

**1582** Cryptographic operation – MAC

1583	Hierarchical to:	No other components
1584	Dependencies:	[FDP_ITC.1 Import of user data without security
1585		attributes, or FDP_ITC.2 Import of user data with
1586		security attributes, or FCS_CKM.1 Cryptographic key
1587		generation]: fulfilled by
1588		FCS_CKM.1/DH_PACE_EAC1PP
1589		FCS_CKM.4 Cryptographic key destruction: fulfilled by

1591 FCS\_COP.1.1/PACE\_MAC\_EAC1PP

1590

1592 The TSF shall perform <u>secure messaging – message authentication code<sup>39</sup> in accordance</u>

FCS\_CKM.4/EAC1PP.

- 1593 with a specified cryptographic algorithm <u>CMAC, Retail-MAC<sup>4041</sup></u> and cryptographic key
- 1594 sizes <u>3DES 112, AES 128, 192, 256</u> bit<sup>4243</sup> that meet the following: <u>compliant to [7]</u><sup>44</sup>.
- 1595 FCS\_CKM.1/CA\_EAC1PP
  - 1596 Cryptographic key generation Diffie-Hellman for Chip Authentication session keys

1597	Hierarchical to:	No other components
1598	Dependencies:	[FCS_CKM.2 Cryptographic key distribution or
1599		FCS_COP.1 Cryptographic operation] fulfilled by

<sup>&</sup>lt;sup>33</sup> [assignment: list of cryptographic operations]

<sup>&</sup>lt;sup>34</sup> [selection: AES, 3DES]

<sup>&</sup>lt;sup>35</sup> [assignment: cryptographic algorithm]

<sup>&</sup>lt;sup>36</sup> [assignment: cryptographic key sizes]

<sup>&</sup>lt;sup>37</sup> [selection: *112, 128, 192, 256*]

<sup>&</sup>lt;sup>38</sup> [assignment: *list of standards*]

<sup>&</sup>lt;sup>39</sup> [assignment: *list of cryptographic operations*]

<sup>&</sup>lt;sup>40</sup> [assignment: *cryptographic algorithm*]

<sup>&</sup>lt;sup>41</sup> [selection: CMAC, Retail-MAC]

<sup>&</sup>lt;sup>42</sup> [assignment: *cryptographic key sizes*]

<sup>43 [</sup>selection: 112, 128, 192, 256]

<sup>44 [</sup>assignment: list of standards]



1600 1601	FCS_COP.1/CA_ENC_EAC1PP and FCS_COP.1/CA_MAC_EAC1PP
1602	FCS_CKM.4 Cryptographic key destruction fulfilled by
1603	FCS_CKM.4/EAC1PP.

# 1604 FCS\_CKM.1.1/CA\_EAC1PP

# 1605 The TSF shall generate cryptographic keys in accordance with a specified cryptographic

1606 key generation algorithm <u>Diffie-Hellman protocol compliant to PKCS#3 and based on an</u>

- 1607 <u>ECDH protocol<sup>45</sup></u> and specified cryptographic key sizes <u>TDES 112, AES 128, 192 and 256</u>
- 1608 <u>bits</u><sup>46</sup> that meet the following: <u>based on the Diffie-Hellman key derivation protocol compliant</u>
- 1609 to [27] and [16], based on an ECDH protocol compliant to [26]<sup>4748</sup>
- 1610 22. Application note (taken from [5], application note 12)

1611 FCS\_CKM.1/CA\_EAC1PP implicitly contains the requirements for the hashing functions used 1612 for key derivation by demanding compliance to [16].

1613 23. Application note (taken from [5], application note 13)

1614 The TOE generates a shared secret value with the terminal during the Chip Authentication 1615 Protocol Version 1, see [16]. This protocol may be based on the Diffie-Hellman-Protocol 1616 compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [27]) or on the 1617 ECDH compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm) (cf. [26], for 1618 details). The shared secret value is used to derive the Chip Authentication Session Keys used 1619 for encryption and MAC computation for secure messaging (defined in Key Derivation Function 1620 [16]).

1621 24. Application note (taken from [5], application note 14)

1622 The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the 1623 keys for secure messaging from any shared secrets of the Authentication Mechanisms. The 1624 Chip Authentication Protocol v.1 may use SHA-1 (cf. [16]). The TOE may implement additional 1625 hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol v.1 (cf. [16] for 1626 details).

1627 25. Application note (taken from [5], application note 15)

1628 The TOE shall destroy any session keys in accordance with FCS\_CKM.4 from [13] after (i) 1629 detection of an error in a received command by verification of the MAC and (ii) after successful 1630 run of the Chip Authentication Protocol v.1. (iii) The TOE shall destroy the PACE Session Keys 1631 after generation of a Chip Authentication Session Keys and changing the secure messaging

1632 to the Chip Authentication Session Keys. (iv) The TOE shall clear the memory area of any

<sup>&</sup>lt;sup>45</sup> [assignment: *cryptographic key generation algorithm*]

<sup>&</sup>lt;sup>46</sup> [assignment: *cryptographic key sizes*]

<sup>&</sup>lt;sup>47</sup> [assignment: *list of standards*]

<sup>&</sup>lt;sup>48</sup> [selection: based on the Diffie-Hellman key derivation protocol compliant to [27] and [16], based on an ECDH protocol compliant to [26]]



session keys before starting the communication with the terminal in a new after-reset-session
as required by FDP\_RIP.1/EAC1PP. Concerning the Chip Authentication keys
FCS\_CKM.4/EAC1PP is also fulfilled by FCS\_CKM.1/CA\_EAC1PP.

- 1636 FCS\_COP.1/CA\_ENC\_EAC1PP
- **1637** Cryptographic operation Symmetric Encryption / Decryption
- 1638 Hierarchical to: No other components
- 1639Dependencies:[FDP\_ITC.1 Import of user data without security1640attributes, or FDP\_ITC.2 Import of user data with1641security attributes, or FCS\_CKM.1 Cryptographic key1642generation] fulfilled by FCS\_CKM.1/CA\_EAC1PP
- 1643FCS\_CKM.4 Cryptographic key destruction fulfilled by1644FCS\_CKM.4/EAC1PP
- 1645 FCS\_COP.1.1/CA\_ENC\_EAC1PP
- 1646 The TSF shall perform <u>secure messaging encryption and decryption<sup>49</sup></u> in accordance 1647 with a specified cryptographic algorithm <u>Triple-DES and AES</u><sup>50</sup> and cryptographic key 1648 sizes <u>Triple-DES:112, AES: 128, 192 and 256 bits</u><sup>51</sup> that meet the following:[16]<sup>52</sup>.
- 1649 26. Application note (taken from [5], application note 16)

1650 This SFR requires the TOE to implement the cryptographic primitives (e.g. Triple-DES and/or 1651 AES) for secure messaging with encryption of the transmitted data. The keys are agreed 1652 between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 1653 according to the FCS\_CKM.1/CA\_EAC1PP.

- 1654 FCS\_COP.1/SIG\_VER\_EAC1PP
- **1655** Cryptographic operation Signature verification by electronic document
- 1656
   Hierarchical to:
   No other components

   1657
   Dependencies:
   [FDP\_ITC.1 Import of user data without security

   1658
   attributes, or FDP\_ITC.2 Import of user data with

   1659
   security attributes, or FCS\_CKM.1 Cryptographic key

   1660
   generation] fulfilled by FCS\_CKM.1/CA\_EAC1PP

<sup>&</sup>lt;sup>49</sup> [assignment: *list of cryptographic operations*]

<sup>&</sup>lt;sup>50</sup> [assignment: *cryptographic algorithm*]

<sup>&</sup>lt;sup>51</sup> [assignment: *cryptographic key sizes*]

<sup>&</sup>lt;sup>52</sup> [assignment: *list of standards*]



1661		FCS_CKM.4 Cryptographic key destruction fulfilled by
1662		FCS_CKM.4/EAC1PP
1663	FCS_COP.1.1/SIG_VER_EAC1PP	
1664	The TSF shall perform digital	signature verification53 in accordance with a specified
1665	cryptographic algorithm <u>RSA v1.</u>	5 with SHA-256 and SHA-512, RSA-PSS with SHA-256
1666	and SHA-512, ECDSA with	<u>SHA-256, SHA-224, SHA-384 and SHA-512<sup>54</sup> and</u>
1667	cryptographic key sizes <u>RSA 20</u>	48, 4096 and from 2000 bit to 4096 bit in one bit steps.
1668	<u>ECDSA 160, 192, 224, 256, 320</u>	<u>, 384, 521 bits<sup>55</sup> that meet the following: [24][29]</u> <sup>56</sup> .
1669	27. Application note (redefined by ST auth	or, taken from [5], application note 17)
1670	Applied.	
1671	28. Application note (from ST author)	
1672 1673 1674	algorithms and cryptographic key size	ctionalities supports RSA and RSA-CRT digital signature es 512 bits up to 4096 bits with equal security measures. gh attack potential an adequate key length must be used.
1675 1676	FCS_COP.1/CA_MAC_EAC1PP Cryptographic operation – MAC	
1677	Hierarchical to:	No other components
1678	Dependencies:	[FDP_ITC.1 Import of user data without security
1679		attributes, or FDP_ITC.2 Import of user data with
1680		security attributes, or FCS_CKM.1 Cryptographic key
1681		generation] fulfilled by FCS_CKM.1/CA_EAC1PP
1682		FCS_CKM.4 Cryptographic key destruction fulfilled by
1683		FCS_CKM.4/EAC1PP

1684 FCS\_COP.1.1/CA\_MAC\_EAC1PP

<sup>&</sup>lt;sup>53</sup> [assignment: *list of cryptographic operations*]
<sup>54</sup> [assignment: *cryptographic algorithm*]
<sup>55</sup> [assignment: *cryptographic key sizes*]
<sup>56</sup> [assignment: *list of standards*]



- 1685 The TSF shall perform <u>secure messaging message authentication code<sup>57</sup> in accordance</u>
- 1686 with a specified cryptographic algorithm <u>CMAC or Retail-MAC<sup>58</sup></u> and cryptographic key
- 1687 sizes <u>112, 128, 192 and 256 bits<sup>59</sup> that meet the following: [16]<sup>60</sup>.</u>

#### 1688 29. Application note (taken from [5], application note 18)

1689 This SFR requires the TOE to implement the cryptographic primitive for secure messaging with 1690 encryption and message authentication code over the transmitted data. The key is agreed 1691 between the TSF by Chip Authentication Protocol Version 1 according to the 1692 FCS\_CKM.1/CA\_EAC1PP. Furthermore, the SFR is used for authentication attempts of a 1693 terminal as Personalisation Agent by means of the authentication mechanism.

- 1694 The following SFRs are defined because the TOE supports the Chip Authentication version 2 1695 and Restricted Identification key pair(s) generation on the TOE as described in 1696 FMT MTD.1/SK PICC EAC2PP.
- 1697 FCS\_CKM.1/CA2
- **1698** Cryptographic key generation Chip Authentication version 2 Key pair(s)
- 1699 Hierarchical to: No other components 1700 **Dependencies:** [FCS\_CKM.2 Cryptographic key distribution or 1701 FCS\_COP.1 Cryptographic operation] fulfilled by FCS COP.1/PACE ENC EAC2PP and 1702 FCS COP.1/PACE MAC EAC2PP 1703 1704 FCS\_CKM.4 Cryptographic key destruction fulfilled by 1705 FCS CKM.4/EAC2PP
- 1706 FCS\_CKM.1.1/CA2

1707The TSF shall generate cryptographic keys to Chip Authentication 2 in accordance with a1708specified cryptographic key generation algorithm RSA or ECC<sup>61</sup> and specified cryptographic1709key sizes 1024, 1280, 1536, 1984, 2048, 3072 and 4096 bits or 160, 192, 224, 256, 384 and1710 $521 \text{ bits}^{62}$  that meet the following: [31]<sup>63</sup>.

- 1711 **30.** Application note (from ST author)
- 1712 The TOE supports to create Chip Authentication version 2 Key pair(s) on the TOE as described
- 1713 in FMT\_MTD.1/SK\_PICC\_EAC2PP. The TOE generates the key pair(s) in secure way, but the

<sup>&</sup>lt;sup>57</sup> [assignment: *list of cryptographic operations*]

<sup>&</sup>lt;sup>58</sup> [assignment: *cryptographic algorithm*]

<sup>&</sup>lt;sup>59</sup> [assignment: *cryptographic key sizes*]

<sup>&</sup>lt;sup>60</sup> [assignment: *list of standards*]

<sup>&</sup>lt;sup>61</sup> [assignment: cryptographic key generation algorithm]

<sup>&</sup>lt;sup>62</sup> [assignment: cryptographic key sizes]

<sup>&</sup>lt;sup>63</sup> [assignment: *list of standards*]



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

## 1716 FCS\_CKM.1/RI

- 1717 Cryptographic key generation Restricted Identification Key pair (s)
- 1718 Hierarchical to: No other components 1719 [FCS\_CKM.2 Cryptographic key distribution or Dependencies: 1720 FCS COP.1 Cryptographic operation] not fullfilled but 1721 justified: the crypgographic part of Restricted 1722 Identification protocol is not part of the TOE, so no 1723 cryptographic operation is related to FCS\_CKM.1/RI. 1724 FCS CKM.4 Cryptographic key destruction fullfilled by 1725 FCS CKM.4/EAC2PP
- 1726 FCS\_CKM.1.1/RI

1727 The TSF shall generate cryptographic keys **to Restricted Identification** in accordance with a 1728 specified cryptographic key generation algorithm <u>RSA or ECC</u><sup>64</sup> and specified cryptographic 1729 key sizes <u>1024</u>, <u>1280</u>, <u>1536</u>, <u>1984</u>, <u>2048</u>, <u>3072</u> and <u>4096</u> bits or <u>160</u>, <u>192</u>, <u>224</u>, <u>256</u>, <u>384</u> and 1730 <u>521 bits</u><sup>65</sup> that meet the following: <u>[31][17]</u><sup>66</sup>.

1731 31. Application note (from ST author)

1732 The TOE supports to create Restricted Identification Key pair(s) on the TOE as described in 1733 FMT\_MTD.1/SK\_PICC\_EAC2PP. The TOE generates the key pair(s) in secure way, but the 1734 appropriate key size shall be assessed during the personalization of the TOE. 1735 The refinement was necessary for the sake of clarity.

1736 The following SFRs are new and concern cryptographic support for ePassport application in 1737 combination with [5] in case the Active Authentication protocol is active:

- 1738 FCS\_CKM.1/AA
- 1739 FCS\_COP.1/AA
- 1740 FCS\_CKM.1/AA
- 1741 Cryptographic key generation Active Authentication Key Pair
- 1742 Hierarchical to:

No other components

<sup>&</sup>lt;sup>64</sup> [assignment: cryptographic key generation algorithm]

<sup>65 [</sup>assignment: cryptographic key sizes]

<sup>66 [</sup>assignment: list of standards]



1743 1744 1745	Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] fulfilled by FCS_COP.1/AA
1746 1747		FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/EAC1PP
1748	FCS_CKM.1.1/AA	
1749 1750 1751 1752	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <u>RSA or ECDSA<sup>67</sup></u> and specified cryptographic key sizes <u>1024, 1280,</u> <u>1536, 1984, 2048, 3072 and 4096 bits or 160, 192, 224, 256, 384 and 521 bits</u> <sup>68</sup> that meet the following: [7][9] <sup>69</sup> .	
1753 1754	FCS_COP.1/AA Cryptographic operation – Active Aut	hentication
1755	Hierarchical to:	No other components
1756 1757 1758 1759	Dependencies:	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attribute or FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/AA
1760 1761		FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/EAC1PP
1762	FCS_COP.1.1/AA	

1763 The TSF shall perform <u>digital signature creation</u><sup>70</sup> in accordance with a specified

- 1764 cryptographic algorithm <u>RSA or ECDSA<sup>71</sup></u> and . cryptographic key sizes <u>RSA with key</u>
- 1765 sizes 2048-4096 and ECDSA with key sizes  $160-521^{72}$  that meet the following: [7][9]<sup>73</sup>.

1766 The following SFRs are new and concerns cryptographic support for ePassport applications in 1767 combination with [5].

- 1768 FCS\_CKM.1/CAM
  - <sup>67</sup> [assignment: cryptographic key generation algorithm]

<sup>68 [</sup>assignment: cryptographic key sizes]

<sup>&</sup>lt;sup>69</sup> [assignment: *list of standards*]

<sup>&</sup>lt;sup>70</sup> [assignment: *list of cryptographic operations*]

<sup>&</sup>lt;sup>71</sup> [assignment: *cryptographic algorithm*]

<sup>&</sup>lt;sup>72</sup> [assignment: *cryptographic key sizes*]

<sup>73 [</sup>assignment: list of standards]

- 1769 FCS\_COP.1/CAM
- 1770 FCS\_CKM.1/CAM
- 1771 Cryptographic key generation PACE-CAM public key and Diffie-Hellman for General Mapping in
   1772 PACE-GM
- Hierarchical to: No other components
  Dependencies: [FCS\_CKM.2 Cryptographic key distribution or
  FCS\_COP.1 Cryptographic operation]
  fulfilled by FCS\_COP.1/CAM
  FCS\_CKM.4 Cryptographic key destruction
  fulfilled by FCS\_CKM.4/EAC1PP
- 1779 FCS\_CKM.1.1/CAM
- 1780 The TSF shall generate cryptographic keys in accordance with a specified cryptographic
- 1781 key generation algorithm <u>PACE-CAM in combination with PACE-GM<sup>74</sup></u> and specified 1782 cryptographic key sizes <u>AES 128, 192 and 256 bit<sup>75</sup></u> that meet the following: [9]<sup>76</sup>.
- 1783 32. Application note (from ST author)

1784 In the combined protocol PACE-CAM, after the completion of PACE in combination with the 1785 general mapping (PACE-GM), the chip authenticates itself by adding (multiplying) the 1786 randomly chosen nonce of the GM step with the inverse of the chip authentication secret key, 1787 and sends this value together with chip authentication public key to the card; cf.[9].

1788 FCS\_COP.1/CAM1789 Cryptographic operation – PACE-CAM

1790	Hierarchical to:	No other components
1791	Dependencies:	[FDP_ITC.1 Import of user data without security
1792		attributes, or FDP_ITC.2 Import of user data with
1793		security attributes, or FCS_CKM.1 Cryptographic key
1794		generation]
1795		fulfilled by FCS_CKM.1/CAM

<sup>&</sup>lt;sup>74</sup> [assignment: cryptographic key generation algorithm]

<sup>&</sup>lt;sup>75</sup> [assignment: *cryptographic key sizes*]

<sup>&</sup>lt;sup>76</sup> [assignment: *list of standards*]



1796	FCS_CKM.4 Cryptographic key destruction
1797	fulfilled by FCS_CKM.4/EAC1PP

# 1798 FCS\_COP.1.1/CAM

- 1799 The TSF shall perform the PACE-CAM protocol<sup>77</sup> in accordance with a specified
- 1800 cryptographic algorithm <u>PACE-CAM<sup>78</sup></u> and cryptographic key sizes <u>AES 128, 192 and 256</u>
- 1801 <u>bits</u><sup>79</sup> that meet the following:  $[9]^{80}$
- 1802 33. Application note (from ST author)

1803 Whereas FCS\_CKM.1/CAM addresses the Diffie-Hellman based key-derivation, this SFR is
1804 concerned with the correct implementation and execution of the whole PACE-CAM protocol.
1805 Note that in particular the last protocol step to authenticate the chip towards the terminal is an
1806 essential part of the protocol, and not addressed in FCS\_CKM.1/CAM.

- 1807 The following SFRs are imported due to claiming [14]. They only concern the cryptographic 1808 support for an eSign application.
- 1809 FCS\_CKM.1/SSCDPP
- 1810 FCS\_CKM.4/SSCDPP
- 1811 (equivalent to FCS\_CKM.4/EAC2PP, but listed here for the sake of completeness)

## 1812 • FCS\_COP.1/SSCDPP

- 1813 FCS\_CKM.1/SSCDPP
- 1814 Cryptographic key generation

1815	Hierarchical to:	No other components
1816 1817	Dependencies:	FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] fulfilled by
1818		FCS_COP.1/SSCDPP
1819		FCS_CKM.4 Cryptographic key destruction fulfilled by
1820		FCS_CKM.4/EAC2PP

1821 FCS\_CKM.1.1/SSCDPP

<sup>&</sup>lt;sup>77</sup> [assignment: *list of cryptographic operations*]

<sup>78 [</sup>assignment: cryptographic algorithm]

<sup>79 [</sup>assignment: cryptographic key sizes]

<sup>&</sup>lt;sup>80</sup> [assignment: *list of standards*]



- 1822 The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic 1823 key generation algorithm <u>RSA or ECDSA<sup>81</sup></u> and specified cryptographic key sizes <u>1024</u>.
- 1824 1280, 1536, 1984, 2048, 3072 and 4096 bits or 160, 192, 224, 256, 384 and 521 bits<sup>82</sup>
- 1825 that meet the following:  $[23]^{83}$ .

## 1826 34. Application note (taken from [14], application note 5)

1827 The ST writer performed the missing operations in the element FCS\_CKM.1.1/SSCDPP. The 1828 refinement in the element FCS\_CKM.1.1 SSCDPP substitutes "cryptographic keys" by 1829 "SCD/SVD pairs" because it clearly addresses the SCD/SVD key generation.

- 1830 FCS\_COP.1/SSCDPP
- 1831 Cryptographic operation
- 1832 Hierarchical to: No other components
- 1833Dependencies:FDP\_ITC.1 Import of user data without security1834attributes, FDP\_ITC.2 Import of user data with security1835attribute or FCS\_CKM.1 Cryptographic key generation]1836fulfilled by FCS\_CKM.1/SSCDPP1837FCS\_CKM.4 Cryptographic key destruction fulfilled by
- 1838 FCS\_CKM.4/EAC2PP

## 1839 FCS\_COP.1.1/SSCDPP

1840The TSF shall perform digital signature creation84 in accordance with a specified1841cryptographic algorithm RSA according to RSASSA-PKCS1-v1\_5, RSASSA-PSS or1842ECDSA according to ISO14883-385 and . cryptographic key sizes RSA with key sizes18432048-4096 and ECDSA with key sizes 160-52186 that meet the following: [24] [29]87.

1844 35. Application note (taken from [14], application note 7)

1845 Applied.

1846 36. Application note (from ST author)

1847 The underlying Platform supports RSA, RSA-CRT and ECDSA digital signature algorithms and 1848 cryptographic key sizes 2048 bits to 4096 bits (RSA) and 160 bits to 521 bits (ECDSA) with

<sup>&</sup>lt;sup>81</sup> [assignment: cryptographic key generation algorithm]

<sup>&</sup>lt;sup>82</sup> [assignment: *cryptographic key sizes*]

<sup>&</sup>lt;sup>83</sup> [assignment: *list of standards*]

<sup>&</sup>lt;sup>84</sup> [assignment: *list of cryptographic operations*]

<sup>&</sup>lt;sup>85</sup> [assignment: *cryptographic algorithm*]

<sup>&</sup>lt;sup>86</sup> [assignment: *cryptographic key sizes*]

<sup>&</sup>lt;sup>87</sup> [assignment: *list of standards*]



- 1849 equal security measures. However, to fend off attackers with high attack potential an adequate1850 key length must be used
- 1851 **6.1.2. Class FIA**
- 1852 Table 10 provides an overview of the authentication and identification mechanisms used.

Name	SFR for the TOE	
PACE protocol	FIA UID.1/PACE EAC2PP	
• • • • • • • •	FIA UAU.5/PACE EAC2PP	
	FIA_AFL.1/Suspend_PIN_EAC2PP	
	FIA_AFL.1/Block_PIN_EAC2PP	
	FIA AFL.1/PACE EAC2PP	
	FIA_AFL.1/PACE_EAC1PP	
PACE-CAM protocol	SFRs above for the PACE part; in addition, for the Chip	
-	Authentication Mapping (CAM):	
	FIA_API.1/PACE_CAM	
	FIA_UAU.5/PACE_EAC1PP	
Terminal Authentication	FIA_UAU.1/EAC2_Terminal_EAC2PP	
Protocol version 2	FIA_UAU.5/PACE_EAC2PP	
Chip Authentication Protocol	FIA_API.1/CA_EAC2PP	
version 2	FIA_UAU.5/PACE_EAC2PP	
	FIA_UAU.6/PACE_EAC2PP	
Terminal Authentication	FIA_UAU.1/PACE_EAC1PP	
Protocol version 1	FIA_UAU.5/PACE_EAC1PP	
Chip Authentication Protocol	FIA_API.1/EAC1PP	
version 1	FIA_UAU.5/PACE_EAC1PP	
	FIA_UAU.6/EAC_EAC1PP	
Active Authentication	FIA_API.1/AA	
	FIA_UAU.1/PACE_EAC1PP	
	FIA_UAU.4/PACE_EAC1PP	
Restricted Identification	FIA_API.1/RI_EAC2PP	
eSign-PIN	FIA_UAU.1/SSCDPP	
Table 10 Overview of authentication and identification SFRs		

1853 1854

6.1.2.1. SFRs for EAC2-protected Data

1855 The following SFRs are imported due to claiming [6]. They mainly concern authentication1856 mechanisms related to applications with EAC2-protected data.

- 1857 FIA\_AFL.1/Suspend\_PIN\_EAC2PP
- 1858 FIA\_AFL.1/Block\_PIN\_EAC2PP
- 1859 **FIA\_API.1/CA\_EAC2PP**
- 1860 FIA\_API.1/RI\_EAC2PP
- 1861 FIA\_UID.1/PACE\_EAC2PP
- 1862 FIA\_UID.1/EAC2\_Terminal\_EAC2PP

1863 37. Application note (taken from [20], application note 10)

1864 The user identified after a successfully performed TA2 protocol is an EAC2 terminal. Note that 1865 TA1 is covered by FIA\_UID.1/PACE\_EAC1PP. In that case, the terminal identified is in addition 1866 also an EAC1 terminal.

- 1867 FIA\_UAU.1/PACE\_EAC2PP
- 1868 FIA\_UAU.1/EAC2\_Terminal\_EAC2PP
- 1869 FIA\_UAU.4/PACE\_EAC2PP
- 1870 38. Application note (taken from [6], application note 26)

For PACE, the TOE randomly selects an almost uniformly distributed nonce of 128 bit length. The [20] and the current ST support a key derivation function based on AES; see [17]. For TA2, the TOE randomly selects a nonce  $r_{PICC}$  of 64 bit length, see [17]. This SFR extends FIA\_UAU.4/PACE\_EAC1PP from [13] by assigning the authentication mechanism Terminal Authentication 2.

- 1876 FIA\_UAU.5/PACE\_EAC2PP
- 1877 FIA\_UAU.6/CA\_EAC2PP
- 1878 FIA\_AFL.1/PACE\_EAC2PP
- 1879 FIA\_UAU.6/PACE\_EAC2PP
- **1880** FIA\_AFL.1/Suspend\_PIN\_EAC2PP
- **1881** Authentication failure handling Suspending PIN
- 1882 Hierarchical to: No other components
  1883 Dependencies: [FIA\_UAU.1 Timing of authentication] fulfilled by
  1884 FIA\_UAU.1/PACE\_EAC2PP
- 1885 FIA\_AFL.1.1/Suspend\_PIN\_EAC2PP
- 1886 The TSF shall detect when <u>an administrator configurable positive integer within [1-127]</u><sup>88</sup>
- 1887 unsuccessful authentication attempts occur related to <u>consecutive failed authentication</u>
- 1888 <u>attempts using the PIN as the shared password for PACE<sup>89</sup>.</u>
- 1889 FIA\_AFL.1.2/Suspend\_PIN\_EAC2PP

<sup>&</sup>lt;sup>88</sup>[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

<sup>&</sup>lt;sup>89</sup> [assignment: *list of authentication events*]



- 1890 When the defined number of unsuccessful authentication attempts has been  $\underline{met}^{90}$ , the
- 1891 TSF shall suspend the reference value of the PIN according to [17]<sup>91</sup>.
- 1892 39. Application note (taken from [6], application note 19)

1893 This SFR is not in conflict to FIA\_AFL.1 from [13], since it just adds a requirement specific to 1894 the case where the PIN is the shared password. Thus, the assigned integer number for 1895 unsuccessful authentication attempts with any PACE password could be different to the integer 1896 for the case when using a PIN.

- 1897 FIA\_AFL.1/Block\_PIN\_EAC2PP1898 Authentication failure handling Blocking PIN
- 1899 Hierarchical to: No other components
- 1900 Dependencies:[FIA\_UAU.1 Timing of authentication] fulfilled by1901FIA\_UAU.1/PACE\_EAC2PP
- 1902 FIA\_AFL.1.1/Block\_PIN\_EAC2PP
- 1903 The TSF shall detect when <u>an administrator configurable positive integer within [1-127]</u><sup>92</sup>
- unsuccessful authentication attempts occur related to <u>consecutive failed authentication</u>
   attempts using the suspended<sup>93</sup> PIN as the shared password for PACE<sup>94</sup>.
- 1906 FIA\_AFL.1.2/Block\_PIN\_EAC2PP
- 1907 When the defined number of unsuccessful authentication attempts has been  $\underline{met}^{95}$ , the 1908 TSF shall block the reference value of PIN according to  $[17]^{96}$ .
- 1909 FIA\_API.1/CA\_EAC2PP
- **1910** Authentication Proof of Identity
- 1911 Hierarchical to: No other components
- 1912 Dependencies: No dependencies
- 1913 FIA\_API.1.1/CA\_EAC2PP

- <sup>92</sup> [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
- <sup>93</sup> as required by FIA\_AFL.1/Suspend\_PIN\_EAC2PP

95 [selection: met, surpassed]

<sup>&</sup>lt;sup>90</sup> [selection: *met*, *surpassed*]

<sup>&</sup>lt;sup>91</sup> [assignment: *list of actions*]

<sup>&</sup>lt;sup>94</sup> [assignment: *list of authentication events*]

<sup>&</sup>lt;sup>96</sup> [assignment: *list of actions*]



- 1914 The TSF shall provide the <u>protocol Chip Authentication 2 according to [17]</u><sup>97</sup>, to prove the 1915 identity of the TOE<sup>98</sup>.
- 1916 FIA\_API.1/RI\_EAC2PP
- **1917** Authentication Proof of Identity
- 1918 Hierarchical to: No other components
- 1919 Dependencies: No dependencies
- 1920 FIA\_API.1.1/RI\_EAC2PP
- 1921 The TSF shall provide the <u>Restricted Identification protocol according to [17]</u><sup>99</sup>, to prove
- 1922 the identity of the  $\underline{TOE}^{100}$ .
- 1923 40. Application note (taken from [6], application note 20)

1924 Restricted Identification provides a sector-specific identifier of every electronic document. It 1925 thus provides a pseudonymous way to identify the Electronic Document Holder in a case where 1926 the CHAT of the terminal does not allow to access Sensitive User Data that directly identify the 1927 Electronic Document Holder. Restricted Identification shall only be used after successfully 1928 running Terminal Authentication 2 and Chip Authentication 2. Note that Restricted Identification 1929 is optional according to [17], and thus the above SFR only applies if Restricted Identification is 1930 supported by the TOE.

- **1931** FIA\_UID.1/PACE\_EAC2PP
- **1932** Timing of identification
- 1933 Hierarchical to: No other components
- 1934 Dependencies: No dependencies
- 1935 FIA\_UID.1.1/PACE\_EAC2PP
- 1936 The TSF shall allow:
- 1937
   1. to establish a communication channel,
   1938
   2. carrying out the PACE protocol according to [17]
   1939
   3. to read the Initialization Data if it is not disabled by TSF according to
   1940
   <u>FMT\_MTD.1/INI\_DIS\_FMT\_MTD.1/INI\_DIS\_EAC2PP^101</u>

<sup>&</sup>lt;sup>97</sup> [assignment: *authentication mechanism*]

<sup>&</sup>lt;sup>98</sup> [assignment: authorised user or role, or of the TOE itself]

<sup>&</sup>lt;sup>99</sup> [assignment: *authentication mechanism*]

<sup>&</sup>lt;sup>100</sup> [assignment: *authorized user or role*]

<sup>&</sup>lt;sup>101</sup> [assignment: *list of TSF-mediated actions*]



1941 4. <u>none<sup>102</sup></u>

1942 on behalf of the user to be performed before the user is identified.

- 1943 FIA\_UID.1.2/PACE\_EAC2PP
- 1944 The TSF shall require each user to be successfully identified before allowing any other
- 1945 TSF-mediated actions on behalf of that user.
- 1946 41. Application note (taken from [6], application note 21)

1947 The user identified after a successful run of PACE is a PACE terminal. In case the PIN or PUK 1948 were used for PACE, the user identified is the Electronic Document Holder using a PACE 1949 terminal. Note that neither the CAN nor the MRZ effectively represent secrets, but are 1950 restricted-revealable; i.e. in case the CAN or the MRZ were used for PACE, it is either the 1951 Electronic Document Holder itself, an authorized person other than the Electronic Document 1952 Holder, or a device.

- **1953 42. Application note (from ST author)**
- 1954 The refinement was necessary to ensure unified terminology usage of SFRs.
- 1955 FIA\_UID.1/EAC2\_Terminal\_EAC2PP1956 Timing of identification
- 1957 Hierarchical to: No other components
- 1958 Dependencies: No dependencies
- 1959 FIA\_UID.1.1/EAC2\_Terminal\_EAC2PP
- 1960 The TSF shall allow
- 1961 1. to establish a communication channel,
- 1962 2. carrying out the PACE protocol according to [17].
- 19633. to read the Initialization Data if it is not disabled by TSF according to1964<u>FMT\_MTD.1/INI\_DIS</u>FMT\_MTD.1/INI\_DIS\_EAC2PP
- 1965 4. carrying out the Terminal Authentication protocol 2 according to [17]<sup>103</sup>
- 1966 5. <u>none<sup>104</sup></u>
- 1967 on behalf of the user to be performed before the user is identified.
- 1968 FIA\_UID.1.2/EAC2\_Terminal\_EAC2PP

<sup>&</sup>lt;sup>102</sup> [assignment: *list of TSF-mediated actions*]

<sup>&</sup>lt;sup>103</sup> [assignment: *list of TSF-mediated actions*]

<sup>&</sup>lt;sup>104</sup> [assignment: *list of TSF-mediated actions*]



- 1969 The TSF shall require each user to be successfully identified before allowing any other
- 1970 TSF-mediated actions on behalf of that user.
- 1971 43. Application note (taken from [6], application note 22)
- 1972 The user identified after a successfully performed TA2 is an EAC2 terminal. The types of EAC2 1973 terminals are application dependent;
- 1974 44. Application note (taken from [6], application note 23)

1975 In the life cycle phase manufacturing, the manufacturer is the only user role known to the TOE.
1976 The manufacturer writes the initialization data and/or pre-personalization data in the audit
1977 records of the IC.

Note that a Personalization Agent acts on behalf of the electronic document issuer under his
and the CSCA's and DS's policies. Hence, they define authentication procedures for
Personalization Agents. The TOE must functionally support these authentication procedures.
These procedures are subject to evaluation within the assurance components ALC\_DEL.1 and
AGD\_PRE.1. The TOE assumes the user role Personalization Agent, if a terminal proves the
respective Terminal Authorization level (e. g. a privileged terminal, cf. [17]).

- 1984 45. Application note (from ST author)
- 1985 The refinement was necessary to ensure unified terminology usage of SFRs.
- **1986** FIA\_UAU.1/PACE\_EAC2PP
- **1987** Timing of authentication
- 1988 Hierarchical to:

No other components

- 1989 Dependencies:[FIA\_UID.1 Timing of identification]: fulfilled by1990FIA\_UID.1/PACE\_EAC2PP
- 1991 FIA\_UAU.1.1/PACE\_EAC2PP
- 1992 The TSF shall allow:
- 1993 1. <u>to establish a communication channel</u>,
- 1994 2. <u>carrying out the PACE protocol according to [17]</u>.
- 19953. to read the Initialization Data if it is not disabled by TSF according to1996FMT\_MTD.1/INI\_DIS\_FMT\_MTD.1/INI\_DIS\_EAC2PP,
- 1997 4. <u>none<sup>105</sup></u>
- 1998 on behalf of the user to be performed before the user is authenticated.
- 1999 FIA\_UAU.1.2/PACE\_EAC2PP

<sup>&</sup>lt;sup>105</sup> [assignment: *list of TSF-mediated actions*]

- 2000 The TSF shall require each user to be successfully authenticated before allowing any other
- 2001 TSF-mediated actions on behalf of that user.
- 2002 46. Application note (taken from [6], application note 24)

2003 If PACE has been successfully performed, secure messaging is started using the derived 2004 session keys (PACE- $K_{MAC}$ , PACE- $K_{Enc}$ ), cf. FTP\_ITC.1/PACE\_EAC2PP. 44. Application note 2005 (taken from [6], application note 23) also applies here.

- 2006 47. Application note (from ST author)
- 2007 The refinement was necessary to ensure unified terminology usage of SFRs.
- FIA\_UAU.1/EAC2\_Terminal\_EAC2PPTiming of authentication
- 2010 Hierarchical to: No other components
- 2011Dependencies:[FIA\_UID.1 Timing of identification]: fulfilled by2012FIA\_UAU.1/EAC2\_Terminal\_EAC2PP
- 2013 FIA\_UAU.1.1/EAC2\_Terminal\_EAC2PP
- 2014 The TSF shall allow:
- 2015 1. <u>to establish a communication channel</u>,
- 2016 2. carrying out the PACE protocol according to [17],
- 2017
   3. to read the Initialization Data if it is not disabled by TSF according to

   2018
   <u>FMT\_MTD.1/INI\_DIS</u>FMT\_MTD.1/INI\_DIS\_EAC2PP
- 2019 4. carrying out the Terminal Authentication protocol 2 according to [17]<sup>106</sup>
- 2020 on behalf of the user to be performed before the user is authenticated.
- 2021 FIA\_UAU.1.2/EAC2\_Terminal\_EAC2PP
- 2022 The TSF shall require each user to be successfully authenticated before allowing any other
- 2023 TSF-mediated actions on behalf of that user.
- 2024 48. Application note (taken from [6], application note 25)

The user authenticated after a successful run of TA2 is an EAC2 terminal. The authenticated 2025 2026 terminal will immediately perform Chip Authentication 2 as required by FIA API.1/CA EAC2PP using, amongst other, Comp(ephem-PK<sub>PCD</sub>-TA) from 2027 the accomplished TA2. Note that Passive Authentication using SO<sub>c</sub> is considered to be part of 2028 2029 CA2 within this ST.

<sup>&</sup>lt;sup>106</sup> [assignment: *list of TSF-mediated actions*]



- 2030 **49.** Application note (from ST author)
- 2031 The refinement was necessary to ensure unified terminology usage of SFRs.
- 2032 FIA\_UAU.4/PACE\_EAC2PP
- **2033** Single-use authentication of the Terminals by the TOE
- 2034 Hierarchical to: No other components
- 2035 Dependencies: No dependencies
- 2036 FIA\_UAU.4.1/PACE\_EAC2PP
- 2037 The TSF shall prevent reuse of authentication data related to:
- 2038 1. <u>PACE protocol according to [17]</u>,
- 2039 2. <u>Authentication Mechanism based on AES<sup>107</sup></u>
- 2040 3. <u>Terminal Authentication 2 protocol according to [17]</u>.<sup>108</sup>
- 2041 4. <u>none<sup>109</sup></u>
- 2042 50. Application note (taken from [6], application note 26)

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

- 2047 FIA\_UAU.5/PACE\_EAC2PP
- 2048 Multiple authentication mechanisms
- 2049 Hierarchical to: No other components
- 2050 Dependencies: No dependencies
- 2051 FIA\_UAU.5.1/PACE\_EAC2PP
- 2052 The TSF shall provide

2055

2056

- 2053 1. PACE protocol according to [17],
- 2054 2. Passive Authentication according to [8]
  - 3. Secure messaging in MAC-ENC mode according to [18]
  - 4. Symmetric Authentication Mechanism based on TDES and AES<sup>110111</sup>

<sup>&</sup>lt;sup>107</sup> [selection: *Triple-DES* , AES or other approved algorithms]

<sup>&</sup>lt;sup>108</sup> [assignment: *identified authentication mechanism*(s)]

<sup>&</sup>lt;sup>109</sup> [assignment: *identified authentication mechanism(s)*]

<sup>&</sup>lt;sup>110</sup> restricting the [selection: *Triple-DES, AES or other approved algorithms*]

<sup>&</sup>lt;sup>111</sup> [selection: *AES or other approved algorithms*]

- Terminal Authentication 2 protocol according to [17], 2057 5. Chip Authentication 2 according to [17]<sup>112113</sup> 6. 2058 none<sup>114</sup> 7. 2059 2060 to support user authentication. 2061 FIA UAU.5.2/PACE EAC2PP 2062 The TSF shall authenticate any user's claimed identity according to the following rules: 2063 1. Having successfully run the PACE protocol the TOE accepts only received 2064 commands with correct message authentication codes sent by secure messaging 2065 with the key agreed with the terminal by the PACE protocol. 2066 2. The TOE accepts the authentication attempt as Personalization Agent by 2067 Symmetric Authentication (Device authentication) according to [30]<sup>115</sup> The TOE accepts the authentication attempt by means of the Terminal 2068 3. 2069 Authentication 2 protocol, only if (i) the terminal presents its static public key PK<sub>PCD</sub> and the key is successfully verifiable up to the CVCA and (ii) the terminal uses the 2070 2071 PICC identifier IDP<sub>ICC</sub> = Comp(ephem-PK<sub>PICC</sub>-PACE) calculated during, and the 2072 secure messaging established by the, current PACE authentication. 4. Having successfully run Chip Authentication 2, the TOE accepts only received 2073 2074 commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by Chip Authentication 2.<sup>116</sup> 2075 none<sup>117</sup> 2076 5.
- 2077 51. Application note (taken from [6], application note 27)

2078 Refinement of FIA\_UAU.5.2/PACE\_EAC2PP, since here PACE must adhere to [17] and [18], 2079 cf. 9. Application note (taken from [6], application note 10). Since the formulation "MAC-ENC 2080 mode" is slightly ambiguous (there is only one secure messaging mode relevant both in [13] 2081 and here, and it is actually the same in both references), it is removed here by refinement in 2082 the third bullet point of FIA\_UAU.5.1/PACE\_EAC2PP.

2083 Remark: Note that 5. and 6. in FIA\_UAU.5.1/PACE\_EAC2PP and 3. and 4. of 2084 FIA\_UAU.5.2/PACE\_EAC2PP are additional assignments (using the open assignment 2085 operation) compared to [13].

2086 52. Application note (from ST author)

 $<sup>^{112}</sup>$  Passive Authentication using SOc is considered to be part of CA2 within this ST.

<sup>&</sup>lt;sup>113</sup> [assignment: *list of multiple authentication mechanisms*]

<sup>&</sup>lt;sup>114</sup> [assignment: *list of multiple authentication mechanisms*]

<sup>&</sup>lt;sup>115</sup> [selection: the Authentication Mechanism with Personalization Agent Key(s)]

<sup>&</sup>lt;sup>116</sup> [assignment: rules describing how the multiple authentication mechanisms provide authentication]

<sup>&</sup>lt;sup>117</sup> [assignment: rules describing how the multiple authentication mechanisms provide authentication]



- 2087 Symmetric Authentication Mechanism implemented according to [30].
- 2088 FIA\_UAU.6/CA\_EAC2PP Re-authenticating of Terminal by the TOE 2089 2090 Hierarchical to: No other components 2091 Dependencies: No dependencies 2092 FIA UAU.6.1/CA EAC2PP The TSF shall re-authenticate the user under the conditions each command sent to the 2093 2094 TOE after a successful run of Chip Authentication 2 shall be verified as being sent by the 2095 EAC2 terminal<sup>118</sup>. 2096 FIA\_AFL.1/PACE\_EAC2PP 2097 Authentication failure handling – PACE authentication using non-blocking authorisation data 2098 Hierarchical to: No other components 2099 Dependencies: [FIA\_UAU.1 Timing of authentication]: fulfilled by 2100 FIA\_UAU.1/PACE\_EAC2PP 2101 FIA\_AFL.1.1/PACE\_EAC2PP 2102 The TSF shall detect when an administrator configurable positive integer number within [1-127]<sup>119</sup> unsuccessful authentication attempt occurs related to <u>authentication attempts</u> 2103 using the PACE password as shared password.<sup>120</sup> 2104 2105 FIA AFL.1.2/PACE EAC2PP
- 2106 When the defined number of unsuccessful authentication attempts has been <u>met<sup>121</sup></u>, the
- 2107 TSF shall <u>delay each following authentication attempt until the next successful</u>
- 2108 <u>authentication.<sup>122</sup></u>.
- 2109 53. Application note (from ST author)
- In line with [6] the shared password for PACE can be CAN, MRZ, PIN and PUK. The specific case of PIN is detailed in FIA\_AFL.1/Suspend\_PIN\_EAC2PP and

<sup>&</sup>lt;sup>118</sup> [assignment: list of conditions under which re-authentication is required]

<sup>&</sup>lt;sup>119</sup> [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

<sup>&</sup>lt;sup>120</sup> [assignment: list of authentication events]

<sup>&</sup>lt;sup>121</sup> [selection: met ,surpassed]

<sup>&</sup>lt;sup>122</sup> [assignment: *list of actions*]



- 2112 FIA\_AFL.1/Block\_PIN\_EAC2PP and furthermore 39. Application note (taken from [6], 2113 application note 19).
- 2114 FIA\_UAU.6/PACE\_EAC2PP
- **2115** Re-authenticating of Terminal by the TOE
- 2116 Hierarchical to: No other components
- 2117 Dependencies: No dependencies
- 2118 FIA\_UAU.6.1/PACE\_EAC2PP
- 2119 The TSF shall re-authenticate the user under the conditions <u>each command sent to the</u>
- 2120 <u>TOE after successful run of the PACE protocol shall be verified as being sent by the PACE</u>
- 2121 <u>terminal.<sup>123</sup></u>
- 2122 6.1.2.2. SFRs for EAC1-protected data
- FIA\_UID.1/PACE\_EAC1PP
- FIA\_UAU.1/PACE\_EAC1PP
- 2125 FIA\_UAU.4/PACE\_EAC1PP
- 2126 FIA\_UAU.5/PACE\_EAC1PP
- 2127 FIA\_UAU.6/PACE\_EAC1PP
- 2128 (equivalent to **FIA\_UAU.6/PACE\_EAC2PP**, but listed here for the sake of completeness)
- **FIA\_UAU.6/EAC\_EAC1PP**
- 2130 FIA\_API.1/EAC1PP
- 2131 FIA\_AFL.1/PACE\_EAC1PP
- 2132 (equivalent to **FIA\_AFL.1/PACE\_EAC2PP**, but listed here for the sake of completeness)
- 2133 FIA\_UID.1/PACE\_EAC1PP
- 2134 Timing of identification
- 2135 Hierarchical to: No other components
- 2136 Dependencies: No dependencies
- 2137 FIA\_UID.1.1/PACE\_EAC1PP
- 2138 The TSF shall allow:

<sup>&</sup>lt;sup>123</sup> [assignment: list of conditions under which re-authentication is required]

2139	1.	to establish the communication channel,
2140	2.	carrying out the PACE Protocol according to [7],
2141	3.	to read the Initialization Data if it is not disabled by TSF according to
2142		FMT_MTD.1/INI_DIS_FMT_MTD.1/INI_DIS_EAC1PP
2143	4.	to carry out the Chip Authentication Protocol v.1 according to [16] or the Chip
2144		Authentication mapping (PACE-CAM) according to [9].
2145	5.	to carry out the Terminal Authentication Protocol v.1 according to [16] resp.

- 2146 according to [9] if PACE-CAM is used.<sup>124</sup>
- 2147 6. <u>none<sup>125</sup></u>.
- 2148 on behalf of the user to be performed before the user isidentified.
- 2149 FIA\_UID.1.2/PACE\_EAC1PP
- 2150 The TSF shall require each user to be successfully identified before allowing any other
- 2151 TSF-mediated actions on behalf of that user.
- 2152 54. Application note (from ST author)

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

2156 55. Application note (taken from [5], application note 20)

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

2159 56. Application note (taken from [5], application note 21)

2160 In the Phase 2 "Manufacturing" the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalisation Data in the audit records of the IC. The 2161 electronic document manufacturer may create the user role Personalisation Agent for transition 2162 from Phase 2 to Phase 3 "Personalisation of the Electronic Document". The users in role 2163 2164 Personalisation Agent identify themselves by means of selecting the authentication key. After 2165 personalisation in the Phase 3 the PACE domain parameters, the Chip Authentication data 2166 and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE 2167 2168 protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may 2169 2170 identify itself as (i) EAC1 terminal by selection of the templates for the Terminal Authentication 2171 Protocol Version 1 or (ii) if necessary and available by authentication as Personalisation Agent 2172 (using the Personalisation Agent Key).

2173 57. Application note (taken from [5], application note 22)

<sup>&</sup>lt;sup>124</sup> [assignment: list of TSF-mediated actions]

<sup>&</sup>lt;sup>125</sup> [assignment: list of TSF-mediated actions]



User identified after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either

- 2176 the electronic document holder itself or an authorised other person or device (PACE terminal).
- 2177 58. Application note (taken from [5], application note 23)
- In the life-cycle phase 'Manufacturing' the Manufacturer is the only user role known to the TOE.
   The Manufacturer writes the Initialisation Data and/or Pre-personalisation Data in the audit
   records of the IC.
- Please note that a Personalisation Agent acts on behalf of the electronic document Issuer
  under his and CSCA and DS policies. Hence, they define authentication procedure(s) for
  Personalisation Agents. The TOE must functionally support these authentication procedures
  being subject to evaluation within the assurance components ALC\_DEL.1 and AGD\_PRE.1.
  The TOE assumes the user role 'Personalisation Agent', when a terminal proves the respective
  Terminal Authorisation Level as defined by the related policy (policies).
- 2187 59. Application note (from ST author)
- 2188 The refinement was necessary to ensure unified terminology usage of SFRs.
- 2189 FIA\_UAU.1/PACE\_EAC1PP2190 Timing of authentication
- 2191 Hierarchical to: No other components
- 2192 Dependencies:FIA\_UID.1 Timing of identification fulfilled by2193FIA\_UID.1/PACE\_EAC1PP
- 2194 FIA\_UAU.1.1/PACE\_EAC1PP
- 2195 The TSF shall allow:
- 2196 1. to establish the communication channel,
- 2197 2. carrying out the PACE Protocol according to [7],
- 21983. to read the Initialization Data if it is not disabled by TSF according to2199FMT MTD.1/INI DIS FMT MTD.1/INI DIS EAC1PP ,
- 2200 4. to identify themselves by selection of the authentication key
- 5. to carry out the Chip Authentication Protocol Version 1 according to [16]
- 2202 6. to carry out the Terminal Authentication Protocol Version 1 according to [16]<sup>126</sup>
- 2203 7. to carry out the Active Authetnication Mechanism according to [9]<sup>127</sup>
- 2204 on behalf of the user to be performed before the user is authenticated.

<sup>&</sup>lt;sup>126</sup> [assignment: *list of TSF-mediated actions*]

<sup>&</sup>lt;sup>127</sup> [assignment: *list of TSF-mediated actions*]


#### 2205 FIA\_UAU.1.2/PACE\_EAC1PP

- 2206 The TSF shall require each user to be successfully authenticated before allowing any other
- 2207 TSF-mediated actions on behalf of that user.
- 2208 60. Application note (taken from [5], application note 24)

The SFR FIA\_UAU.1/PACE\_EAC1PP in the current ST covers the definition in [13] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to [13].

2212 61. Application note (taken from [5], application note 25)

The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets but are restricted revealable; i.e. it is either the electronic document holder itself or an authorised another person or device (PACE terminal).

If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-K<sub>MAC</sub>, PACE-K<sub>Enc</sub>), cf. FTP\_ITC.1/PACE\_EAC1PP.

- 2219 62. Application note (from ST author)
- 2220 The refinement was necessary to ensure unified terminology usage of SFRs.
- **2221** FIA\_UAU.4/PACE\_EAC1PP
- 2222 Single-use authentication mechanisms Single-use authentication of the Terminal by the TOE
- 2223 Hierarchical to: No other components
- 2224 Dependencies: No dependencies
- 2225 FIA\_UAU.4.1/PACE\_EAC1PP
- 2226 The TSF shall prevent reuse of authentication data related to
- 2227 1. PACE Protocol according to [7],
- 2228 2. <u>Authentication Mechanism based on Triple-DES or AES<sup>128</sup></u>
- 2229 3. <u>Terminal Authentication Protocol v.1 according to [16]</u>.<sup>129</sup>
- 2230 4. <u>Active Authentication protocol according to [7], [9]</u>
- 2231 63. Application note (taken from [5], application note 26)

The SFR FIA\_UAU.4.1/PACE\_EAC1PP in the current ST covers the definition in [13] and extends it by the EAC aspect 3. This extension does not conflict with the strict conformance to

extends it by the EAC aspect 3. This extension does not conflict with the strict conformance to [13]. The generation of random numbers (random nonce) used for the authentication protocol

<sup>&</sup>lt;sup>128</sup> [selection: *Triple-DES, AES or other approved algorithms*]

<sup>&</sup>lt;sup>129</sup> [assignment: *identified authentication mechanism(s)*]

- (PACE) and Terminal Authentication as required by FIA\_UAU.4/PACE\_EAC1PP is requiredby FCS\_RND.1 from [13].
- 2237 64. Application note (taken from [5], application note 27)

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

- 2243 65. Application note (ST author)
- The refinement was necessary because the authentication data (nonce) is must not be reused during Active Authentication protocol according to [9].
- **2246** FIA\_UAU.5/PACE\_EAC1PP
- 2247 Multiple authentication mechanisms
- 2248 Hierarchical to: No other components
- 2249 Dependencies: No dependencies
- 2250 FIA\_UAU.5.1/PACE\_EAC1PP
- 2251 The TSF shall provide
- 1. <u>PACE Protocol according to [7]</u> and PACE-CAM protocol according to [9]
- 2253 2. <u>Passive Authentication according to [8]</u>
- 2254 3. <u>Secure messaging in MAC-ENC mode according to [7].</u>
- 2255 4. <u>Symmetric Authentication Mechanism based on Triple-DES or AES<sup>130</sup></u>
- 2256 5. <u>Terminal Authentication Protocol v.1 according to [16], 131</u>
- 2257 to support user authentication
- 2258 FIA\_UAU.5.2/PACE\_EAC1PP
- 2259 The TSF shall authenticate any user's claimed identity according to the <u>following rules</u>:
- 22601. Having successfully run the PACE protocol the TOE accepts only received2261commands with correct message authentication code sent by means of secure2262messaging with the key agreed with the terminal by means of the PACE protocol.

<sup>&</sup>lt;sup>130</sup> [selection: *Triple-DES, AES or other approved algorithms*]

<sup>&</sup>lt;sup>131</sup> [assignment: *list of multiple authentication mechanism*]

2263	2.	The TOE accepts the authentication attempt as Personalisation Agent by the
2264		Symmetric Authentication (Device authentication) according to [30] <sup>132</sup>
2265	3.	After run of the Chip Authentication Protocol Version 1 the TOE accepts only
2266		received commands with correct message authentication code sent by means of
2267		secure messaging with key agreed with the terminal by means of the Chip
2268		Authentication Mechanism v1.
2269	4.	The TOE accepts the authentication attempt by means of the Terminal
2270		Authentication Protocol v.1 only if the terminal uses the public key presented during
2271		the Chip Authentication Protocol v.1 and the secure messaging established by the
2272		Chip Authentication Mechanism v.1. or if the terminal uses the public key
2273		presented during PACE-CAM and the secure messaging established during

- 2274 **PACE.**<sup>133</sup>
- 2275 5. <u>none</u><sup>134</sup>
- 2276 66. Application note (from ST author)

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

2280 67. Application note (taken from [5], application note 28)

The SFR FIA\_UAU.5.1/PACE\_EAC1PP in the current ST covers the definition in [13] and extends it by EAC aspects 4), 5), and 6). The SFR FIA\_UAU.5.2/PACE\_EAC1PP in the current ST covers the definition in [13] and extends it by EAC aspects 2), 3), 4) and 5). These extensions do not conflict with the strict conformance to [13].

- 2285 FIA\_UAU.6/EAC\_EAC1PP
- **2286** Re-authenticating Re-authenticating of Terminal by the TOE
- 2287 Hierarchical to: No other components
- 2288 Dependencies: No dependencies
- 2289 FIA\_UAU.6.1/EAC\_EAC1PP
- 2290 The TSF shall re-authenticate the user under the conditions each command sent to the
- 2291 <u>TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as</u>
- 2292 being sent by the Inspection System.<sup>135</sup>

<sup>&</sup>lt;sup>132</sup> [selection: the Authentication Mechanism with Personalisation Agent Key(s)]

<sup>&</sup>lt;sup>133</sup> [assignment: rules describing how the multiple authentication mechanisms provide authentication ]

<sup>&</sup>lt;sup>134</sup> [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

<sup>&</sup>lt;sup>135</sup> [assignment: list of conditions under which re-authentication is required]

#### 2293 68. Application note (taken from [5], application note 29)

The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [8] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC\_ENC mode each command based on a corresponding MAC algorithm whether it was sent by the successfully authenticated terminal (see FCS\_COP.1/CA\_MAC\_EAC1PP for further details). The TOE does not execute any command with incorrect message authentication code.

- Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user.
- 2302 FIA\_API.1/EAC1PP
- 2303Authentication Proof of Identity
- 2304 Hierarchical to: No other components
- 2305 Dependencies: No dependencies
- 2306 FIA\_API.1.1/EAC1PP
- 2307 The TSF shall provide a <u>Chip Authentication Protocol Version 1 according to  $[16]^{136}$  to 2308 prove the identity of the <u>TOE</u>.<sup>137</sup></u>
- 2309 69. Application note (taken from [5], application note 30)

This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [16]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or ECDH) and two session keys for secure messaging in ENC\_MAC mode according to [8]. The terminal verifies by means of secure messaging whether the electronic document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

- 2316 The following SFR is newly defined in this ST and addresses the PACE-CAM protocol.
- 2317 FIA\_API.1/PACE\_CAM
- 2318 Authentication Proof of Identity
- 2319 Hierarchical to: No other components
- 2320 Dependencies: No dependencies
- 2321 FIA\_API.1.1/PACE\_CAM
- 2322 The TSF shall provide a protocol PACE-CAM [9]<sup>138</sup> to prove the identity of the <u>TOE</u>.<sup>139</sup>

<sup>&</sup>lt;sup>136</sup> [assignment: *authentication mechanism*]

<sup>&</sup>lt;sup>137</sup> [assignment: *authorized user or role*]

<sup>&</sup>lt;sup>138</sup> [assignment: *authentication mechanism*]

<sup>&</sup>lt;sup>139</sup> [assignment: *authorized user or role, or of the TOE itself*]



- 2323 The following SFR is newly defined in this ST and addresses the Active Authentication 2324 protocol:
- 2325 FIA\_API.1/AA2326 Authentication Proof of Identity
- 2327 Hierarchical to: No other components
- 2328 Dependencies: No dependencies
- 2329 FIA\_API.1.1/AA
- 2330 The TSF shall provide a <u>Active Authentication protocol according to [7] [9]</u><sup>140</sup> to prove the 2331 identity of the <u>TOE</u>.<sup>141</sup>
- 2332 The following SFRs are imported due to claiming [14]. They concern access mechanisms for
- an eSign application, if available.
- FIA\_UID.1/SSCDPP
- 2335 FIA\_AFL.1/SSCDPP
- 2336 FIA\_UID.1/SSCDPP2337 Timing of identification
- 2338 Hierarchical to: No other components
- 2339 Dependencies: No dependencies
- 2340 FIA\_UID.1.1/SSCDPP
- 2341 The TSF shall allow
- 2342 1. <u>Self-test according to FPT\_TST.1 FPT\_TST.1/SSCDPP</u>,
- 2343 2. <u>none<sup>142</sup></u>
- 2344 on behalf of the user to be performed before the user is identified
- 2345 FIA\_UID.1.2/SSCDPP

<sup>&</sup>lt;sup>140</sup> [assignment: *authentication mechanism*]

<sup>&</sup>lt;sup>141</sup> [assignment: authorized user or role, or of the TOE itself]

<sup>&</sup>lt;sup>142</sup> [assignment: *list of additional TSF-mediated actions*]



- The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
- 2348 70. Application note (taken from [14], application note 11)
- 2349 Applied.
- 2350 71. Application note (from ST author)
- 2351 The refinement was necessary to ensure unified terminology usage of SFRs.
- 2352 FIA\_AFL.1/SSCDPP
- 2353Authentication failure handling
- 2354 Hierarchical to:
- 2355 Dependencies: FIA\_UAU.1 Timing of Authentication fulfilled by 2356 FIA\_UAU.1/SSCDPP

No other components

- 2357 FIA\_AFL.1.1/SSCDPP
- The TSF shall detect when <u>an administrator configurable positive integer within 3-15<sup>143</sup></u> unsuccessful authentication attempts occur related to <u>consecutive failed authentication</u> attempts.<sup>144</sup>
- 2361 FIA\_AFL.1.2/SSCDPP
- When the defined number of unsuccessful authentication attempts has been <u>met<sup>145</sup></u>, the TSF shall <u>block RAD<sup>146</sup></u>.
- 2364 72. Application note (taken from [14], application note 13)
- 2365 Applied
- 2366 6.1.2.3. SFRs for eSign-applications
- 2367 FIA\_UAU.1/SSCDPP
- 2368Timing of authentication
- 2369 Hierarchical to:

No other components

<sup>&</sup>lt;sup>143</sup> [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

<sup>&</sup>lt;sup>144</sup> [assignment: *list of authentication events*]

<sup>&</sup>lt;sup>145</sup> [selection: *met ,surpassed*]

<sup>&</sup>lt;sup>146</sup> [assignment: *list of actions*]



2370 2371	Dependencies: FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/SSCDPP		
2372	FIA_UAU.1.1/SSCDPP		
2373	The TSF shall allow		
2374	1. self test according to FPT_TST.1/SSCD FPT_TST.1/SSCDPP,		
2375	2. identification of the user by means of TSF required by FIA_UID.1/SSCD		
2376	FIA_UID.1/SSCDPP,		
2377	3. establishing a trusted channel between CGA and the TOE by means of TSF		
2378	required by FPT_ITC.1/CA_EAC2 FTP_ITC.1/CA_EAC2PP,		
2379	4. establishing a trusted channel between HID and the TOE by means of TSF		
2380	required by FPT_ITC.1/CA_EAC2 FTP_ITC.1/CA_EAC2PP,		
2381	5. <u>none</u> <sup>147</sup>		
2382	on behalf of the user to be performed before the user is authenticated.		
2383	FIA_UAU.1.2/SSCDPP		
2384	The TSF shall require each user to be successfully authenticated before allowing any other		
2385	TSF-mediated actions on behalf of that user.		
2386	73. Application note (from ST author)		
2387	The refinement was necessary to ensure unified terminology usage of SFRs.		
2388	6.1.3. Class FDP		
2389	Multiple iterations of FDP_ACF.1 exist from imported PPs to define the access control SFPs		
2390	for (common) user data, EAC1-protected user data, and EAC2-protected user data. The		
2391	access control SFPs defined in FDP_ACF.1/EAC1PP from [5] and FDP_ACF.1/EAC2PP from		
2392	[6] are unified in [20] to one single FDP_ACF.1/TRM, whereas the several iterations of		
2393	FDP_ACF.1 from [14] stand separate. [20] takes FDP_ACF.1/EAC2PP as a base definition of		

- functional elements, and it is refined in a way that it is compatible with FDP\_ACF.1/EAC1PP.
  Hence highlighting refers to changes w.r.t. to FDP\_ACF.1/EAC2PP. In the application note
- 2396 below, how FDP\_ACF.1/EAC1PP is covered as well is explained.

<sup>&</sup>lt;sup>147</sup> [assignment: *list of additional TSF-mediated actions*]



2397 Concerning FDP\_ACF.1/TRM in [20] and the several iterations FDP\_ACF.1 from [14], [20] 2398 remarks that FDP\_ACF.1/TRM also concerns data and objects for signature generation. Note 2399 however, that FDP\_ACF.1/TRM requires that prior to granting access to the signature 2400 application, in which the access controls defined in [14] apply, an EAC2 terminal and the 2401 Electronic Document Holder need to be authenticated. Hence, no inconsistency exists.

#### 2402 FDP\_ACF.1/TRM

2403 Security attribute based access control – Terminal Access

2404	Hierarchical to:	No other components
2405 2406 2407	Dependencies:	FDP_ACC.1 Subset access control fulfilled by FDP_ACC.1/TRM_EAC1PP and FDP_ACC.1/TRM_EAC2PP
2408 2409		FMT_MSA.3 Static attribute initialization not fulfilled, but <b>justified</b> :
2410 2411 2412 2413 2414		The access control TSF according to FDP_ACF.1/TRM uses security attributes having been defined during the personalization and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.
2415	FDP_ACF.1.1/TRM	
2416	The TSF shall enforce the Acce	ss Control SFP <sup>148</sup> to objects based on the following:
2417	1) <u>Subjects:</u>	

- 2417 1) Subjects:
- 2418 a) <u>Terminal,</u>
- b) <u>PACE terminal,</u>
- 2420
   c) EAC2 terminal Authentication Terminal and Signature Terminal according to

   2421
   [17]<sup>149</sup>,
- 2422 d) EAC1 terminal;<sup>150</sup>
- 2423 2) <u>Objects:</u>

<sup>&</sup>lt;sup>148</sup> [assignment: *access control SFP*]

<sup>&</sup>lt;sup>149</sup> [assignment: *list of EAC2 terminal types*]

<sup>&</sup>lt;sup>150</sup> [assignment: list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or name groups of SFP-relevant security attributes] (added using open assignment of [6])



2424	a) all user data stored in the TOE; including sensitive EAC1-protected user	
2425	data, and sensitive EAC2-protected user data.	
2426	b) all TOE intrinsic secret (cryptographic) data	
2427	3) <u>Security attributes:</u>	
2428	a) Terminal Authorization Level (access rights)	
2429	b) Authentication status of the Electronic Document Holder as a signatory (if an	
2430	eSign application is included). <sup>151152</sup>	
2431	FDP_ACF.1.2/TRM	
2432	The TSF shall enforce the following rules to determine if an operation among controlled	
2433	subjects and controlled objects is allowed:	
2434	A PACE terminal is allowed to read data objects from FDP_ACF.1/TRM after successful	
2435		
2436	FIA_UAU.1/PACE_EAC2PP or FIA_UAU.1/PACE_EAC1PP. <sup>153</sup>	
2437	FDP_ACF.1.3/TRM	
2437 2438	FDP_ACF.1.3/TRM The TSF shall explicitly authorize access of subjects to objects based on the following	
2438	The TSF shall explicitly authorize access of subjects to objects based on the following	
2438 2439	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none</u> . <sup>154</sup>	
2438 2439 2440	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none</u> . <sup>154</sup> FDP_ACF.1.4/TRM	
2438 2439 2440 2441	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none</u> . <sup>154</sup> FDP_ACF.1.4/TRM The TSF shall explicitly deny access of subjects to objects based on the following	
2438 2439 2440 2441 2442	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none</u> . <sup>154</sup> FDP_ACF.1.4/TRM The TSF shall explicitly deny access of subjects to objects based on the following additional rules:	
2438 2439 2440 2441 2442 2443	<ul> <li>The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none</u>.<sup>154</sup></li> <li>FDP_ACF.1.4/TRM</li> <li>The TSF shall explicitly deny access of subjects to objects based on the following additional rules:</li> <li>1. <u>Any terminal not being authenticated as a PACE terminal or an EAC2 terminal or</u></li> </ul>	
2438 2439 2440 2441 2442 2443 2444	<ul> <li>The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.<sup>154</sup></li> <li>FDP_ACF.1.4/TRM</li> <li>The TSF shall explicitly deny access of subjects to objects based on the following additional rules:</li> <li>1. Any terminal not being authenticated as a PACE terminal or an EAC2 terminal or an EAC1 terminal is not allowed to read, to write, to modify, or to use any user</li> </ul>	

<sup>&</sup>lt;sup>151</sup> [assignment: list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or name groups of SFP-relevant security attributes] (added using open assignment of [6]) <sup>152</sup> [assignment: list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or name groups of SFP-relevant security attributes] (all bullets in FDP\_ACF.1.1/TRM w.r.t. [2]) <sup>153</sup> [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects] <sup>154</sup> [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]

<sup>&</sup>lt;sup>155</sup> note that authentication of an EAC1 or EAC2 terminal to a TOE in certified mode implies a prior run of PACE.



2448	3.	No subject is allowed to read 'Electronic Document Communication Establishment
2449		Authorization Data' stored on the electronic document
2450	4.	No subject is allowed to write or modify 'Secret Electronic Document Holder
2451		Authentication Data' stored on the electronic document, except for PACE terminals
2452		or EAC2 terminals executing PIN management based on the following rules:
2453		1. <u>CAN change</u>
2454		2. <u>Change PIN</u>
2455		3. <u>Resume PIN</u>
2456		4. <u>Unblock PIN</u>
2457		5. <u>Activate PIN</u>
2458		6. Deactivate PIN according to [17]. <sup>156</sup>
2459	5.	No subject is allowed to read, write, modify, or use the private Restricted
2460		Identification key(s) and Chip Authentication key(s) stored on the electronic
2461		document.
2462	6.	Reading, modifying, writing, or using Sensitive User Data that are protected only
2463		by EAC2, is allowed only to EAC2 terminals using the following mechanism:
2464		The TOE applies the EAC2 protocol (cf. <b>FIA UAU.5</b>
2465		FIA_UAU.5/PACE_EAC2PP) to determine access rights of the terminal
2466		according to [17]. To determine the effective authorization of a terminal, the
2467		chip must calculate a bitwise Boolean 'and' of the relative authorization
2468		contained in the CHAT of the Terminal Certificate, the referenced DV
2469		Certificate, and the referenced CVCA Certificate, and additionally the confined
2470		authorization sent as part of PACE. Based on that effective authorization and
2471		the terminal type drawn from the CHAT of the Terminal Certificate, the TOE
2472		shall grant the right to read, modify or write Sensitive User Data, or perform
2473		operations using these Sensitive User Data.
2474	7.	No subject is allowed to read, write, modify or use the data objects 2b) of
2475		FDP_ACF.1/TRM.
2476	8.	No subject is allowed to read Sensitive User Data that are protected only by EAC1,
2477		except an EAC1 terminal (OID inspection system) after EAC1, cf.
2478		FIA_UAU.1/EAC1_FIA_UAU.1/PACE_EAC1PP, that has a corresponding relative
2479		authorization level. This includes in particular EAC1-protected user data DG3 and
2480		DG4 from an ICAO-compliant ePass application, cf. [16] and [8].

<sup>&</sup>lt;sup>156</sup> [assignment: list of rules for PIN management chosen from [17]]

- 9. If Sensitive User Data is protected both by EAC1 and EAC2, no subject is allowed
   to read those data except EAC1 terminals or EAC2 terminals that access these
   data according to rule 6 or rule 8 above.
- 2484 10. Nobody is allowed to read the private signature key(s).<sup>157</sup>

#### 2485 74. Application note (from ST author)

The [20] uses the 'Electronic Document Communication Establishment Authorization Data' expression in 3.1.1.2 Secondary Assets and "Communication Establishment Authorization Data" in FDP\_ACF.1.4/TRM 3. In order to provide consistency in our ST, we use only the Electronic Document Communication Establishment Authorization Data.

2490 75. Application note (taken from [20], application note 11)

2491 The above definition is based on FDP\_ACF.1/TRM\_EAC2PP. We argue that it covers 2492 FDP\_ACF.1/TRM\_EAC1PP as well. Subject 1b and 1d are renamed here from 2493 FDP ACF.1.1/TRM EAC1PP according to Table 1 Objects in 2), in particular the term EAC1-2494 protected user data, subsume all those explicitly enumerated in FDP ACF.1.1/TRM EAC1PP. Also, the security attribute 3a) Terminal Authorization Level here subsumes the explicitly 2495 2496 enumerated attributes 3a) and 3b) of FDP\_ACF.1.1/TRM\_EAC1PP, but are semantically the same. Since in addition EAC2 protected data are stored in the TOE of this ST, additional 2497 2498 subjects, objects and security attributes are listed here. However, since they apply to data with 2499 a different protection mechanism (EAC2), strict conformance is not violated.

FDP\_ACF.1.2/TRM uses the renaming of Table 1 , and references in addition [17]. However the references are compatible as justified in [6], yet both are mentioned here since [17] is the primary norm for an eID application, whereas [7] is normative for an ICAO compliant ePass application. Investigating the references reveals that access to data objects defined in FDP\_ACF.1.1/TRM must be granted if these data are neither EAC1-protected, nor EAC2protected.

- 2506 FDP\_ACF.1.3/TRM is the same as in FDP\_ACF.1.3/TRM\_EAC2PP.
- 2507 References are changed in FDP\_ACF.1.2/TRM\_EAC1PP. It is already justified in [6] that definitions in [17] and [8] are compatible.
- 2509 FDP\_ACF.1.3/TRM is taken over from [5] and [6] (same formulation in both).

Rules 1 and 2 of FDP\_ACF.1.4/TRM\_EAC1PP in [5] are covered by their counterparts rule 1 and rule 2 here. Rules 3 and 4, and rule 6 of FDP\_ACF.1.4/TRM\_EAC1PP in [5] are combined here to rule 8, where terminals need the corresponding CHAT to read data groups. Rule 5 of [5] is here equivalent to rule 7. None of this conflict with strict conformance to [5]. Note that adding additional rules compared to FDP\_ACF.1.4/TRM\_EAC1PP here can never violate strict conformance, as these are rules that explicitly deny access of subjects to objects. Hence security is always increased.

The above definition also covers FDP\_ACF.1.1/TRM\_EAC2PP and extends it by additional subjects and objects. Sensitive User Data in the definition of FDP\_ACF.1.1/TRM\_EAC2PP are here EAC2-protected Sensitive User Data. EAC1-protected data are added here by

<sup>&</sup>lt;sup>157</sup> [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]



- refinement. Since the protection level and mechanisms w.r.t. to EAC2-protected data do not change, strict conformance is not violated.
- FDP\_ACF.1.2/TRM\_EAC2PP and FDP\_ACF.1.3/TRM\_EAC2PP are equivalent to the current definition.
- Rules 8, 9 and 10 are added here by open assignment from [6]. None of these conflicts with strict conformance.
- 2526 The dependency this SFR is met by FDP ACC.1/TRM EAC1PP of and FDP ACC.1/TRM EAC2PP. Note that the SFR in [5] applies the assignment operation, 2527 whereas in [6] (by referencing [13]) the assignment is left open. Hence, they are compatible. 2528 We remark that in order to restrict the access to user data as defined in the SFR 2529 FDP\_ACC.1/TRM\_EAC1PP, clearly access to objects 2b) of FDP\_ACF.1.1/TRM must be 2530 restricted as well according to the SFP, otherwise access to user data is impossible to enforce. 2531
- 2532 76. Application note (from ST author)
- 2533 The refinements were necessary to ensure unified terminology usage of SFRs.
- 2534 The following SFRs are imported due to claiming [6]. They concern access control mechanisms
- 2535 related to EAC2-protected data.
- FDP\_ACC.1/TRM\_EAC2PP
- This SFR is equivalent to/covered by **FDP\_ACC.1/TRM\_EAC1PP**; cf the 75. Application note (taken from [20], application note 11).
- 2539 **FDP\_ACF.1/TRM\_EAC2PP**
- 2540 This is SFR is equivalent to/covered by **FDP\_ACF.1/TRM.**
- 2541 FDP\_RIP.1/EAC2PP
- **FDP\_UCT.1/TRM\_EAC2PP**
- **FDP\_UIT.1/TRM\_EAC2PP**
- 2544 FDP\_ACC.1/TRM\_EAC2PP2545 Subset access control Terminal Access
- 2546 Hierarchical to: No other components
- 2547Dependencies:FDP\_ACF.1 Security attribute based access control:2548fulfilled by FDP\_ACF.1/TRM
  - 2549 FDP\_ACC.1.1/TRM\_EAC2PP

## 

The TSF shall enforce the Access Control SFP<sup>158</sup> on terminals gaining access to the User 2550 Data stored in the travel document electronic document<sup>159</sup> and none<sup>160</sup>. 2551 2552 77. Application note (taken from [20]) This SFR is equivalent to/covered by FDP\_ACC.1/TRM\_EAC1PP; cf.75. Application note 2553 2554 (taken from [20], application note 11). 2555 78. Application note (from ST author) 2556 The refinement was necessary to ensure unified terminology usage as described in Table 1 Overview of identifiers of current ST and PPs. 2557 FDP RIP.1/EAC2PP 2558 2559 Subset residual information protection 2560 Hierarchical to: No other components 2561 Dependencies: No dependencies 2562 FDP\_RIP.1.1\_EAC2PP 2563 The TSF shall ensure that any previous information content of a resource is made unavailable upon the <u>deallocation of the resource from</u><sup>161</sup> the following objects: 2564 2565 1. <u>Session keys (PACE-K<sub>MAC</sub>, PACE-K<sub>Enc</sub>), (CA2-K<sub>MAC</sub>, CA2-K<sub>Enc</sub>) (immediately after</u> closing related communication session), 2566 2. the ephemeral private key ephem-SK<sub>PICC</sub>-PACE (by having generated a DH shared 2567 secret K), 2568 2569 3. Secret Electronic Document Holder Authentication Data, e.g. PIN and/or PUK (when their temporarily stored values are not used any more )<sup>162,</sup> 2570 none.163 2571 4.

#### 2572 79. Application note (taken from [6], application note 30)

The functional family FDP\_RIP possesses such a general character, that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-Data; in this respect it is similar to the functional family FPT\_EMS. Applied to cryptographic keys, FDP\_RIP.1/EAC2PP requires a certain quality metric (*any previous information content of a resource is made* 

<sup>&</sup>lt;sup>158</sup> [assignment: access control SFP]

<sup>&</sup>lt;sup>159</sup> [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

<sup>&</sup>lt;sup>160</sup> [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

<sup>&</sup>lt;sup>161</sup> [selection: allocation of the resource to, deallocation of the resource from]

<sup>&</sup>lt;sup>162</sup> [assignment: *list of objects*]

<sup>&</sup>lt;sup>163</sup> [assignment: *list of objects*]



- *unavailable*) for key destruction in addition to FCS\_CKM.4/EAC2PP that merely requires to ensure key destruction according to a method/standard.
- 2579 Application note 80 (from ST author)
- The above SFR is slightly refined from [20] in order not to confuse Chip Authentication 1 with Chip Authentication 2.
- 2582 FDP\_UCT.1/TRM\_EAC2PP
- **2583** Basic data exchange confidentiality MRTD
- 2584 Hierarchical to:
- 2585Dependencies:[FTP\_ITC.1 Inter-TSF trusted channel, or FTP\_TRP.12586Trusted path] fulfilled by FTP\_ITC.1/PACE\_EAC2PP

No other components

- 2587[FDP\_ACC.1 Subset access control, or FDP\_IFC.12588Subset information flow control] fulfilled by2589FDP\_ACC.1/TRM\_EAC2PP
- 2590 FDP\_UCT.1.1/TRM\_EAC2PP
- The TSF shall enforce the <u>Access Control SFP<sup>164</sup></u> to be able to <u>transmit and receive<sup>165</sup></u> user data in a manner protected from unauthorised disclosure.
- 2593 FDP\_UIT.1/TRM\_EAC2PP
- 2594 TRM Data exchange integrity
- 2595 Dependencies: [FTP\_ITC.1 Inter-TSF trusted channel, or FTP\_TRP.1 2596 Trusted path] fulfilled by FTP\_ITC.1/PACE\_EAC2PP 2597 [FDP ACC.1 Subset access control, or FDP IFC.1 2598 Subset information flow control] fulfilled by FDP\_ACC.1/TRM\_EAC2PP 2599
- 2600 FDP\_UIT.1.1/TRM\_EAC2PP
- 2601 The TSF shall enforce the <u>Access Control SFP</u><sup>166</sup> to be able to <u>transmit and receive</u><sup>167</sup> 2602 user data in a manner protected from <u>modification</u>, <u>deletion</u>, <u>insertion and replay</u><sup>168</sup> errors.

<sup>&</sup>lt;sup>164</sup> [assignment: access control SFP(s) and/or information flow control SFP(s)]

<sup>&</sup>lt;sup>165</sup> [selection: *transmit, receive*]

<sup>&</sup>lt;sup>166</sup> [assignment: access control SFP(s) and/or information flow control SFP(s)]

<sup>&</sup>lt;sup>167</sup> [selection: *transmit, receive*]

<sup>&</sup>lt;sup>168</sup> [selection: *modification, deletion, insertion, replay*]

2603 FDP\_UIT.1.2/TRM\_EAC2PP

- 2604 The TSF shall be able to determine on receipt of user data, whether <u>modification, deletion,</u> 2605 <u>insertion and replay<sup>169</sup></u> has occurred.
- 2606 The following SFRs are imported due to claiming [5]. They concern access control mechanisms 2607 related to EAC1-protected data.

#### 2608 • FDP\_ACC.1/TRM\_EAC1PP

- 2609 The above is equivalent **FDP\_ACC.1/TRM\_EAC2PP**, since EF.SOD (cf. FDP\_ACC.1/TRM in 2610 [5]) can be considered user data.; cf. also the application note below FDP\_ACF.1/TRM.
- 2611 FDP\_ACF.1/TRM\_EAC1PP
- 2612 The above is covered by **FDP\_ACF.1/TRM**; cf. Application Note there.
- 2613 FDP\_RIP.1/EAC1PP
- 2614 **FDP\_UCT.1/TRM\_EAC1PP**
- 2615 (equivalent to **FDP\_UCT.1/TRM\_EAC2PP**, but listed here for the sake of completeness)
- 2616 **FDP\_UIT.1/TRM\_EAC1PP**
- 2617 (equivalent to FDP\_UIT.1/TRM\_EAC2PP, but listed here for the sake of completeness)
- 2618 FDP\_RIP.1/EAC1PP
- 2619 Subset residual information protection
- 2620 Hierarchical to: No other components
- 2621 Dependencies: No dependencies
- 2622 FDP\_RIP.1.1/EAC1PP
- The TSF shall ensure that any previous information content of a resource is made unavailable upon the <u>deallocation of the resource from</u><sup>170</sup> the following objects:
- 2625 1. <u>Session Keys (immediately after closing related communication session)</u>,

<sup>&</sup>lt;sup>169</sup> [selection: *modification, deletion, insertion, replay*]

<sup>&</sup>lt;sup>170</sup> [selection: allocation of the resource to, deallocation of the resource from]



2626 2627 2628	$\frac{1}{27} = \frac{1}{27} \frac{1}{172} \frac{1}$	lenerated a DH shared	
2629 2630		ncern access control	
2631	• FDP_ACC.1/SCD/SVD_Generation_SSCDPP		
2632	• FDP_ACF.1/SCD/SVD_Generation_SSCDPP		
2633	• FDP_ACC.1/SVD_Transfer_SSCDPP		
2634	• FDP_ACF.1/SVD_Transfer_SSCDPP		
2635	• FDP_ACC.1/Signature-creation_SSCDPP		
2636	• FDP_ACF.1/Signature-creation_SSCDPP		
2637	• FDP_RIP.1/SSCDPP		
2638	• FDP_SDI.2/Persistent_SSCDPP		
2639	• FDP_SDI.2/DTBS_SSCDPP		
2640 2641	FDP_ACC.1/SCD/SVD_Generation_SSCDPP Subset access control		
2642	2 Hierarchical to: No other components		
2643	3 Dependencies: FDP_ACF.1 Security attribute I	based access control	
2644	4 fulfilled	by	
2645	5 FDP_ACF.1/SCD/SVD_Generation	on_SSCDPP	
2646	FDP_ACC.1.1/SCD/SVD_Generation_SSCDPP		
2647	7 The TSF shall enforce the <u>SCD/SVD Generation SFP</u> <sup>174</sup> on		
2648	8 1. <u>subjects: S.User,</u>		
2649	9 2. <u>objects: SCD, SVD,</u>		
2650	3. <u>operations: generation of SCD/SVD pair.</u> <sup>175</sup>		
2651 2652	- , ,		

<sup>&</sup>lt;sup>171</sup> according to [7]
<sup>172</sup> [assignment: *list of objects*]
<sup>173</sup> [assignment: *list of objects*]
<sup>174</sup> [assignment: access control SFP]
<sup>175</sup> [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]



2653	Hierarchical to:	No other components	
2654	Dependencies:	FDP_ACC.1 Subset access control fulfilled by	
2655		FDP_ACC.1/SCD/SVD_Generation_SSCDPP	
2656		FMT_MSA.3 Static attribute initialisation fulfilled by	
2657		FMT_MSA.3/SSCDPP	
2658	FDP_ACF.1.1/SCD/SVD_Generatio	on_SSCDPP	
2659	The TSF shall enforce the <u>SCD/</u>	SVD Generation SFP <sup>176</sup> to objects based on the following:	
2660	the user S.User is associated w	ith the security attribute "SCD/SVD Management".177	
2661	FDP_ACF.1.2/SCD/SVD_Generation_SSCDPP		
2662	The TSF shall enforce the following rules to determine if an operation among controlled		
2663	subjects and controlled objects is allowed: <u>S.User with the security attribute "SCD/SVD</u>		
2664	Management" set to "authorised" is allowed to generate SCD/SVD pair. <sup>178</sup>		
2665	FDP_ACF.1.3/SCD/SVD_Generation_SSCDPP		
2666	The TSF shall explicitly authorise access of subjects to objects based on the following		
2667	additional rules: none.179		
2668	FDP_ACF.1.4/SCD/SVD_Generatio	on_SSCDPP	
2669	The TSF shall explicitly deny	access of subjects to objects based on the following	
2670	additional rules: S.User with th	e security attribute "SCD/SVD management" set to "not	
2671	authorised" is not allowed to generate SCD/SVD pair.180		
2672	EDD ACC 1 (CVD Transfer SCODD		

- 2672 FDP\_ACC.1/SVD\_Transfer\_SSCDPP
- 2673 Subset access control
- 2674 Hierarchical to: No other components

 <sup>&</sup>lt;sup>176</sup> [assignment: access control SFP]
 <sup>177</sup> [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]

<sup>&</sup>lt;sup>178</sup> [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

<sup>&</sup>lt;sup>179</sup> [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

<sup>&</sup>lt;sup>180</sup> [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]



2675 2676	Dependencies:	FDP_ACF.1 Security attribute based access control fulfilled by FDP_ACF.1/SVD_Transfer_SSCDPP
2677	FDP_ACC.1.1/SVD_Transfer_SSCE	)PP
2678	The TSF shall enforce the SVD	Transfer SFP <sup>181</sup> on
2679 2680 2681	<ol> <li><u>subjects: S.User,</u></li> <li><u>objects: SVD</u></li> <li><u>operations: export.</u><sup>182</sup></li> </ol>	
2682 2683	FDP_ACF.1/SVD_Transfer_SSCDPP Security attribute based access contro	bl
2684	Hierarchical to:	No other components
2685 2686	Dependencies:	FDP_ACC.1 Subset access control fulfilled by FDP_ACC.1/SVD_Transfer_SSCDPP
2687 2688		FMT_MSA.3 Static attribute initialisation fulfilled by FMT_MSA.3/SSCDPP
2689	FDP_ACF.1.1/SVD_Transfer_SSCDPP	
2690	The TSF shall enforce the SVD Transfer SFP <sup>183</sup> to objects based on the following:	
2691 2692		
2693	FDP_ACF.1.2/SVD_Transfer_SSCDPP	
2694 2695	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: <u><b>R.Admin</b></u> <sup>185</sup> is allowed to export SVD. <sup>186</sup>	

FDP\_ACF.1.3/SVD\_Transfer\_SSCDPP 2696

 <sup>&</sup>lt;sup>181</sup> [assignment: access control SFP]
 <sup>182</sup> [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
 <sup>183</sup> [assignment: access control SFP]

 <sup>&</sup>lt;sup>184</sup> [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]
 <sup>185</sup> [selection: *R.Admin, R.Sigy*]

<sup>&</sup>lt;sup>186</sup> [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]



- 2697 The TSF shall explicitly authorise access of subjects to objects based on the following 2698 additional rules: <u>none</u>.<sup>187</sup>
- 2699 FDP\_ACF.1.4/SVD\_Transfer\_SSCDPP
- 2700 The TSF shall explicitly deny access of subjects to objects based on the following 2701 additional rules: none.<sup>188</sup>
- 2702 81. Application note (taken from [14], application note 9)
- 2703 Applied.
- 2704 FDP\_ACC.1/Signature-creation\_SSCDPP
- 2705 Subset access control
- 2706 Hierarchical to: No other components
- 2707Dependencies:FDP\_ACF.1 Security attribute based access control2708fulfilled by FDP\_ACF.1/Signature-creation\_SSCDPP
- 2709 FDP\_ACC.1.1/Signature\_Creation
- 2710 The TSF shall enforce the <u>Signature Creation SFP<sup>189</sup> on</u>
- 2711 1. <u>subjects: S.User</u>,
- 2712 2. <u>objects: DTBS/R, SCD,</u>
- 2713 3. <u>operations: signature creation.</u><sup>190</sup>
- 2714 FDP\_ACF.1/Signature-creation\_SSCDPP
- 2715 Security attribute based access control

2716	Hierarchical to:	No other components
2717 2718	Dependencies:	FDP_ACC.1 Subset access control fulfilled by FDP_ACC.1/Signature-creation_SSCDPP
2719 2720		FMT_MSA.3 Static attribute initialisation fulfilled by FMT_MSA.3/SSCDPP

2721 FDP\_ACF.1.1/Signature\_Creation\_SSCDPP

<sup>&</sup>lt;sup>187</sup> [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

<sup>&</sup>lt;sup>188</sup> [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

<sup>&</sup>lt;sup>189</sup> [assignment: *access control SFP*]

<sup>&</sup>lt;sup>190</sup> [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]



2722 The TSF shall enforce the <u>Signature Creation SFP<sup>191</sup></u> to objects based on the following:

- 1. <u>the user S.User is associated with the security attribute "Role" and</u>
- 2724 2. <u>the SCD with the security attribute "SCD Operational".<sup>192</sup></u>
- 2725 FDP\_ACF.1.2/Signature\_Creation\_SSCDPP
- The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: <u>R.Sigy is allowed to create electronic</u> <u>signatures for DTBS/R with SCD which security attribute "SCD operational" is set to</u> <u>"yes".<sup>193</sup></u>
- 2730 FDP\_ACF.1.3/Signature\_Creation\_SSCDPP
- The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.<sup>194</sup>
- 2733 FDP\_ACF.1.4/Signature\_Creation\_SSCDPP
- 2734 The TSF shall explicitly deny access of subjects to objects based on the following
- additional rules: <u>S.User is not allowed to create electronic signatures for DTBS/R with SCD</u>
   which security attribute "SCD operational" is set to "no".<sup>195</sup>
- 2737 FDP\_RIP.1/SSCDPP
- 2738 Subset residual information protection
- 2739 Hierarchical to: No other components
- 2740 Dependencies: No dependencies
- 2741 FDP\_RIP.1.1\_SSCDPP
- The TSF shall ensure that any previous information content of a resource is made unavailable upon the <u>de-allocation of the resource from</u><sup>196</sup> the following objects: <u>SCD</u><sup>197</sup>.

<sup>&</sup>lt;sup>191</sup> [assignment: access control SFP]

<sup>&</sup>lt;sup>192</sup> [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]

<sup>&</sup>lt;sup>193</sup> [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

<sup>&</sup>lt;sup>194</sup> [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

<sup>&</sup>lt;sup>195</sup> [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

<sup>&</sup>lt;sup>196</sup> [selection: *allocation of the resource to, deallocation of the resource from*]

<sup>&</sup>lt;sup>197</sup> [assignment: *list of objects*]

- 2744 FDP\_SDI.2/Persistent\_SSCDPP2745 Stored data integrity monitoring and action
- 2746 Hierarchical to: FDP\_SDI.1 Stored data integrity monitoring
- 2747 Dependencies: No dependencies
- 2748 FDP\_SDI.2.1/Persistent\_SSCDPP
- 2749 The TSF shall monitor user data stored in containers controlled by the TSF for integrity
- 2750 <u>error<sup>198</sup> on all objects, based on the following attributes: integrity checked stored data<sup>199</sup>.</u>
- 2751 FDP\_SDI.2.2/Persistent\_SSCDPP
- 2752 Upon detection of a data integrity error, the TSF shall
- 2753 1. prohibit the use of the altered data
- 2754 2. <u>inform the S.Sigy about integrity error.</u><sup>200</sup>
- 2755 82. Application note (taken from [14])
- 2756 The [14] was defined the followings:
- The following data persistently stored by the TOE shall have the user data attribute "integrity checked persistent stored data":
- 2759 1) SCD
- 2760 2) SVD (if persistently stored by the TOE).
- The DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data"
- 2763 FDP\_SDI.2/DTBS\_SSCDPP
- 2764 Stored data integrity monitoring and action
- 2765 Hierarchical to: FDP\_SDI.1 Stored data integrity monitoring
- 2766 Dependencies: No dependencies
- 2767 FDP\_SDI.2.1/DTBS\_SSCDPP

<sup>&</sup>lt;sup>198</sup> [assignment: *integrity errors*]

<sup>&</sup>lt;sup>199</sup> [assignment: user data attributes]

<sup>&</sup>lt;sup>200</sup> [assignment: *action to be taken*]



- 2768 The TSF shall monitor user data stored in containers controlled by the TSF for <u>integrity</u>
- 2769 <u>error<sup>201</sup></u> on all objects, based on the following attributes: <u>integrity checked stored DTBS.</u><sup>202</sup>
- 2770 FDP\_SDI.2.2/DTBS\_SSCDPP
- 2771 Upon detection of a data integrity error, the TSF shall
- 2772 1. prohibit the use of the altered data
- 2773 2. <u>inform the S.Sigy about integrity error.<sup>203</sup></u>
- 2774 83. Application note (taken from [14], application note 10)
- The integrity of TSF data like RAD shall be protected to ensure the effectiveness of the user authentication. This protection is a specific aspect of the security architecture (cf. ADV\_ARC.1).
- 2778 **6.1.4. Class FTP**
- 2779 The following SFRs are imported from [6].
- FTP\_ITC.1/PACE\_EAC2PP
- 2781 **FTP\_ITC.1/CA\_EAC2PP**
- 2782 FTP\_ITC.1/PACE\_EAC2PP2783 Inter-TSF trusted channel after PACE
- 2784 Hierarchical to: No other components
- 2785 Dependencies: No dependencies
- 2786 FTP\_ITC.1.1/PACE\_EAC2PP
- 2787 The TSF shall provide a communication channel between itself and another trusted IT
- 2788 product a PACE terminal that is logically distinct from other communication channels and
- 2789 provides assured identification of its end points and protection of the channel data from
- 2790 modification or disclosure. The trusted channel shall be established by performing the
- 2791 **PACE protocol according to [17]**.
- 2792 FTP\_ITC.1.2/PACE\_EAC2PP

<sup>&</sup>lt;sup>201</sup> [assignment: *list of objects*]

<sup>&</sup>lt;sup>202</sup> [assignment: user data attributes]

<sup>&</sup>lt;sup>203</sup> [assignment: *action to be taken*]



- 2793 The TSF shall permit <u>another trusted IT product</u> **a PACE terminal**<sup>204</sup> to initiate 2794 communication via the trusted channel.
- 2795 FTP\_ITC.1.3/PACE\_EAC2PP
- 2796 The TSF shall initiate enforce communication via the trusted channel for any data
- 2797 <u>exchange between the TOE and a PACE terminal after PACE</u>.<sup>205</sup>
- 2798 84. Application note (taken from [6], application note 31)

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

- 2803 FTP\_ITC.1/CA\_EAC2PP2804 Inter-TSF trusted channel after CA2
- 2805 Hierarchical to: No other components
- 2806 Dependencies: No dependencies
- 2807 FTP\_ITC.1.1/CA2\_EAC2PP

The TSF shall provide a communication channel between itself and another trusted IT product an EAC2 terminal that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. The trusted channel shall be established by performing the CA2 protocol according to [17].

- 2813 FTP\_ITC.1.2/CA2\_EAC2PP
- 2814 The TSF shall permit <u>another trusted IT product</u> an EAC2 terminal<sup>206</sup> to initiate 2815 communication via the trusted channel.
- 2816 FTP\_ITC.1.3/CA2\_EAC2PP
- 2817The TSF shall initiate enforce communication via the trusted channel for any data2818exchange between the TOE and an EAC2 terminal after Chip Authentication 2.207

<sup>&</sup>lt;sup>204</sup> [selection: *the TSF, another trusted IT product*]

<sup>&</sup>lt;sup>205</sup> [assignment: list of functions for which a trusted channel is required]

<sup>&</sup>lt;sup>206</sup> [selection: *the TSF, another trusted IT product*]

<sup>&</sup>lt;sup>207</sup> [assignment: list of functions for which a trusted channel is required]



2819 85. Application note (taken from [6], application note 32)

The trusted channel is established after successful performing the PACE protocol (FIA\_UAU.1/PACE\_EAC2PP), the TA2 protocol (FIA\_UAU.1/EAC2\_Terminal\_EAC2PP) and the CA2 protocol (FIA\_API.1/CA\_EAC2PP). If Chip Authentication 2 was successfully performed, secure messaging is immediately restarted using the derived session keys (CA-K<sub>MAC</sub>, CA-K<sub>Enc</sub>)208. This secure messaging enforces the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS\_COP.1/PACE\_ENC\_EAC2PP and FCS\_COP.1/PACE\_MAC\_EAC2PP.

- 2827 The following SFR is imported due to claiming [5]. It concerns applications with EAC1-2828 protected data
- 2828 protected data.
- FTP\_ITC.1/PACE\_EAC1PP
- 2830 FTP\_ITC.1/PACE\_EAC1PP2831 Inter-TSF trusted channel after PACE
- 2832 Hierarchical to: No other components
- 2833 Dependencies: No dependencies
- 2834 FTP\_ITC.1.1/PACE\_EAC1PP

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

- 2839 FTP\_ITC.1.2/PACE\_EAC1PP
- 2840 The TSF shall permit another trusted IT product to initiate communication via the trusted 2841 channel.
- 2842 FTP\_ITC.1.3/PACE\_EAC1PP
- 2843 The TSF shall initiate enforce communication via the trusted channel for <u>any data</u> 2844 <u>exchange between the TOE and the Terminal.<sup>209</sup></u>

<sup>&</sup>lt;sup>208</sup> otherwise secure messaging is continued using the established PACE session keys, cf. FTP\_ITC.1/PACE\_EAC1PP

<sup>&</sup>lt;sup>209</sup> [assignment: list of functions for which a trusted channel is required]



#### 2845 **6.1.5. Class FAU**

2846 The following SFR is imported due to claiming [6]. It concerns applications with EAC2-2847 protected data.

- 2848 **FAU\_SAS.1/EAC2PP**
- 2849 FAU\_SAS.1/EAC2PP2850 Audit storage
- 2851 Hierarchical to: No other components
- 2852 Dependencies: No dependencies
- 2853 FAU\_SAS.1.1\_EAC2PP
- 2854 The TSF shall provide <u>the Manufacturer<sup>210</sup></u> with the capability to store <u>the Initialisation and</u> 2855 <u>Pre-Personalisation Data<sup>211</sup></u> in the audit records.
- 2856 The following SFR is imported due to claiming [5]. It concerns applications with EAC1-2857 protected data.

#### 2858 • FAU\_SAS.1/EAC1PP

- 2859 (equivalent to FAU\_SAS.1/EAC2PP, but listed here for the sake of completeness)
- 2860 6.1.6. Class FMT
- 2861 FMT\_SMR.1
- 2862Security roles
- 2863Hierarchical to:No other components2864Dependencies:FIA\_UID.1Timing of identification: fulfilled by2865FIA\_UID.1/PACE\_EAC1PP,2866FIA\_UID.1/PACE\_EAC2PP,2867FIA\_UID.1/EAC2\_Terminal\_EAC2PP
- 2868 FMT\_SMR.1.1

<sup>&</sup>lt;sup>210</sup> [assignment: *authorised users*]

<sup>&</sup>lt;sup>211</sup> [assignment: list of management functions to be provided by the TSF]



2869	The T	SF shall maintain the roles
2870	1. <u>Manufacturer,</u>	
2871	2.	Personalization Agent,
2872	3.	Country Verifying Certification Authority (CVCA),
2873	4.	Document Verifier (DV),
2874	5.	Terminal,
2875	6.	PACE Terminal,
2876	7.	EAC2 terminal, if the eID, ePassport and/or eSign application are active,
2877	8.	EAC1 terminal, if the ePassport application is active,
2878	9.	Electronic Document Holder. <sup>212</sup>
2879	FMT_SMF	R.1.2
2880	The T	SF shall be able to associate users with roles.
2881	The next S	SFRs are imported from [6]. They concern mainly applications with EAC2-protected
2882	data.	
2883	• FN	IT_MTD.1/CVCA_INI_EAC2PP
2884	• FN	IT_MTD.1/CVCA_UPD_EAC2PP
2885	• FM	IT_SMF.1/EAC2PP
2886	• FMT_SMR.1/PACE_EAC2PP	
2887	This SFR	is combined with FMT_SMR.1/PACE_EAC1PP into to by <b>FMT_SMR.1</b> .
2888	• FM	IT_MTD.1/DATE_EAC2PP
2889	• FN	IT_MTD.1/PA_EAC2PP
2890	• FM	IT_MTD.1/SK_PICC_EAC2PP
2891	• FM	IT_MTD.1/KEY_READ_EAC2PP
2892	• FN	IT_MTD.1/Initialize_PIN_EAC2PP
2893	• FN	IT_MTD.1/Change_PIN_EAC2PP
2894	• FM	IT_MTD.1/Resume_PIN_EAC2PP
2895	• FN	IT_MTD.1/Unblock_PIN_EAC2PP
2896	• FN	IT_MTD.1/Activate_PIN_EAC2PP
2897	• FN	IT_MTD.3/EAC2PP

<sup>&</sup>lt;sup>212</sup> [assignment: the authorized identified roles]

2898	• FMT_LIM.1/EAC2PP		
2899	86. Application note (taken from [20], application note 12)		
2900	The above SFR concerns the whole	TOE, not just applications with EAC2-protected data.	
2901	• FMT_LIM.2/EAC2PP		
2902	87. Application note (taken from [20], app	lication note 13)	
2903	The above SFR concerns the whole	TOE, not just applications with EAC2-protected data.	
2904	• FMT_MTD.1/INI_ENA_EAC2	2PP	
2905	• FMT_MTD.1/INI_DIS_EAC2	PP	
2906 2907	FMT_MTD.1/CVCA_INI_EAC2PP Management of TSF data – Initialization of CVCA Certificate and Current Date		
2908	Hierarchical to:	No other components	
2909 2910	Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1/EAC2PP	
2911		FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/	
2912		EAC2PP	
2913	FMT_MTD.1.1/CVCA_INI_EAC2PP		
2914	The TSF shall restrict the ability to write <sup>213</sup> the		
2915	1. initial CVCA Public Key,		
2916	2. meta-data of the initial CVCA Certificate as required in [17], resp. [18],		
2917	3. initial Current Date.		
2918	4. <u>none</u> <sup>214</sup>		
2919	to the Personalization Agent.2152	16 <sub>.</sub>	
2920	88. Application note (taken from [6], appli	cation note 36)	

<sup>&</sup>lt;sup>213</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

 <sup>&</sup>lt;sup>214</sup> [assignment: *list of TSF data*]
 <sup>215</sup> [assignment: *the authorized identified roles*]
 <sup>216</sup> [selection: *the manufacturer, the personalization agent*]



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

#### 2924 FMT\_MTD.1/CVCA\_UPD\_EAC2PP

#### 2925 Management of TSF data – Country Verifying Certification Authority

- 2926Hierarchical to:No other components
- 2927 Dependencies:FMT\_SMF.1 Specification of management functions:2928fulfilled by FMT\_SMF.1/EAC2PP
- 2929FMT\_SMR.1Securityroles:fulfilledby2930FMT\_SMR.1/PACE\_EAC2PP
- 2931 FMT\_MTD.1.1/CVCA\_UPD\_EAC2PP
- 2932 The TSF shall restrict the ability to <u>update<sup>217</sup></u> the
- 2933 1. <u>CVCA Public Key (PK<sub>CVCA</sub>),</u>
- 2934 2. meta-data of the CVCA Certificate as required by [17], resp. [18],<sup>218</sup>
- 2935 3. <u>none<sup>219</sup></u>
- 2936 to the Country Verifying Certification Authority.<sup>220</sup>
- 2937 89. Application note (taken from [6], application note 37)

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

- 2941 FMT\_SMF.1/EAC2PP2942 Specification of Management Functions
- 2943 Hierarchical to: No other components
- 2944 Dependencies: No dependencies
- 2945 FMT\_SMF.1.1/EAC2PP
- 2946 The TSF shall be capable of performing the following management functions:

<sup>&</sup>lt;sup>217</sup> [selection: *change\_default, query, modify, delete, clear, [assignment: other operations]*]

<sup>&</sup>lt;sup>218</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>219</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>220</sup> [assignment: *the authorized identified roles*]

IDentity Applet v3.4/eIDAS Security Target



2947	1. Initialization,		
2948	2. Pre-Personalization,	2. <u>Pre-Personalization</u> ,	
2949	3. Personalization,	3. <u>Personalization</u> ,	
2950	4. Configuration,		
2951	5. <u>Resume and unblock t</u>	he PIN (if any),	
2952	6. Activate and deactivate	e the PIN (if any). <sup>221</sup>	
2953	90. Application note (taken from [6], appli	ication note 33)	
2954	The capability of PIN management g	gives additional security to the TOE.	
2955	91. Application note (taken from [6], appli	ication note 34)	
2956 2957 2958 2959 2960 2961	management functionality can only use a commonly shared secret (such as the MRZ – in the case of an ID document – or the CAN) during execution of PACE to control access to sensitive information. A PIN however must not be shared and thus can be kept secret by the user. Hence, this refinement of FMT_SMF.1/EAC2PP increases protection of user data by allowing		
2962 2963	FMT_MTD.1/DATE_EAC2PP Management of TSF data – Current date		
2964	Hierarchical to:	No other components	
2965 2966	Dependencies:	FMT_SMF.1 Specification of management functions fulfilled by FMT_SMF.1/EAC2PP	
2967		FMT_SMR.1 Security roles fulfilled by	
2968		FMT_SMR.1/PACE_EAC2PP	
2969	FMT_MTD.1.1/DATE_EAC2PP		
2970	The TSF shall restrict the ability to modify <sup>222</sup> the current date <sup>223</sup> to		
2971	1. <u>CVCA,</u>		
2972	2. Document Verifier,		
2973	3. EAC2 terminal (Authentic	cation Terminal and Signature Terminal <sup>224</sup> ) possessing an	
2974	Accurate Terminal Certif	icate according to [18].225	

<sup>&</sup>lt;sup>221</sup> [assignment: list of management functions to be provided by the TSF]

<sup>&</sup>lt;sup>222</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>223</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>224</sup> [assignment: *list of EAC2 terminal types*]

<sup>&</sup>lt;sup>225</sup> [assignment: the authorized identified roles]

- 2975 4. <u>none<sup>226</sup></u>
- 2976 92. Application note (taken from [6], application note 38)

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

- **2982** FMT\_MTD.1/PA\_EAC2PP
- 2983 Management of TSF data Personalization Agent
- 2984Hierarchical to:No other components2985Dependencies:FMT\_SMF.1 Specification of management functions2986fulfilled by FMT\_SMF.1/EAC2PP
- 2987FMT\_SMR.1Securityrolesfulfilledby2988FMT\_SMR.1/PACE\_EAC2PP
- 2989 FMT\_MTD.1.1/PA\_EAC2PP

### 2990 The TSF shall restrict the ability to <u>write<sup>227</sup></u> the <u>card/chip security object(s) (SO<sub>c</sub>) and</u>

- 2991 <u>the document Security Object (SO<sub>D</sub>)<sup>228</sup> to the Personalization Agent<sup>229</sup>.</u>
- 2992 93. Application note (taken from [6], application note 39)

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

2996 FMT\_MTD.1/SK\_PICC\_EAC2PP

**2997** Management of TSF data – Chip Authentication and Restricted Identification Private Key(s)

2998	Hierarchical to:	No other components
2999 3000	Dependencies:	FMT_SMF.1 Specification of management functions fulfilled by FMT_SMF.1/EAC2PP
3001		FMT_SMR.1 Security roles fulfilled by
3002		FMT_SMR.1/PACE_EAC2PP

<sup>&</sup>lt;sup>226</sup> [assignment: the authorized identified roles]

<sup>&</sup>lt;sup>227</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>228</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>229</sup> [assignment: *the authorized identified roles*]



#### 3003 FMT\_MTD.1.1/SK\_PICC\_EAC2PP

- 3004 The TSF shall restrict the ability to <u>create or load</u><sup>230231</sup> the <u>Chip Authentication private</u>
- 3005 key(s) (SK<sub>PICC</sub>) and the Restricted Identification Private Key(s)<sup>232</sup> to the Personalization

#### 3006 <u>Agent or the Manufacturer.</u><sup>233</sup>

- 3007 94. Application note (taken from [6], application note 40)
- 3008 Applied, see FCS\_CKM.1/CA2 and FCS\_CKM.1/RI.
- 3009 95. Application note (from ST author)

3010 The FMT\_MTD.1/SK\_PICC\_EAC2PP was refined, because the Manufactuer means here the 3011 electronic document manufacturer, which may create the application and the file system as 3012 well. So the Manufacturer may generate or load the private keys.

- **3013** FMT\_MTD.1/KEY\_READ\_EAC2PP
- 3014 Management of TSF data Private Key Read
- 3015 Hierarchical to:
- 3016Dependencies:FMT\_SMF.1Specification of management functions3017fulfilled by FMT\_SMF.1/EAC2PP

No other components

- 3018FMT\_SMR.1Securityrolesfulfilledby3019FMT\_SMR.1/PACE\_EAC2PP
- 3020 FMT\_MTD.1.1/KEY\_READ\_EAC2PP
- 3021 The TSF shall restrict the ability to <u>read</u><sup>234</sup> the
- 3022 1. PACE passwords,
- 3023 2. <u>Personalization Agent Keys.</u>
- 3024 3. the Chip Authentication private key(s) (SK<sub>PICC</sub>)
- 3025 4. <u>the Restricted Identification private key(s)</u><sup>235</sup>
- 3026 5. <u>none<sup>236</sup></u>

<sup>&</sup>lt;sup>230</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>231</sup> [selection: create, load]

<sup>&</sup>lt;sup>232</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>233</sup> [assignment: the authorized identified roles]

<sup>&</sup>lt;sup>234</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>235</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>236</sup> [assignment: *list of TSF data*]

3027	to <u>none</u> <sup>237</sup>	
3028	96. Application note (taken from [6], application note 41)	
3029	FMT_MTD.1/KEY_READ_EAC2PP extends the SFR from [13] by additional assignments.	
3030 3031	FMT_MTD.1/Initialize_PIN_EAC2PP PIN Management of TSF data – Initialize PIN	
3032	Hierarchical to:	No other components
3033 3034	Dependencies:	FMT_SMF.1 Specification of management functions fulfilled by FMT_SMF.1/EAC2PP
3035 3036		FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/PACE_EAC2PP
3037	FMT_MTD.1.1/Initialize_PIN_EAC2PP	
3038 3039	The TSF shall restrict the ability to <u>write<sup>238</sup> the initial PIN and PUK<sup>239</sup> to the Personalization</u> <u>Agent<sup>240</sup></u>	
3040 3041	FMT_MTD.1/Change_PIN_EAC2PP Management of TSF data – Changing PIN	
3042	Hierarchical to:	No other components
3043 3044	Dependencies:	FMT_SMF.1 Specification of management functions fulfilled by FMT_SMF.1/EAC2PP
3045 3046		FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/PACE_EAC2PP
3047	FMT_MTD.1.1/Change_PIN_EAC2PP	
3048	The TSF shall restrict the ability to change <sup>241</sup> the blocked PIN <sup>242</sup> to	
3049	1. Electronic Document Holder (using the PUK) with unauthenticated terminal	

<sup>&</sup>lt;sup>237</sup> [assignment: *the authorized identified roles*]

<sup>&</sup>lt;sup>238</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>239</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>240</sup> [assignment: the authorized identified roles]

<sup>&</sup>lt;sup>241</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>242</sup> [assignment: *list of TSF data*]



# 3050 2. Authentication Terminal with the Terminal Authorisation level for PIN management 3051 according to [17].<sup>243244</sup>

#### **3052** FMT\_MTD.1/Resume\_PIN\_EAC2PP

3053 Management of TSF data – Resuming PIN

3054	Hierarchical to:	No other components
3055 3056	Dependencies:	FMT_SMF.1 Specification of management functions fulfilled by FMT_SMF.1/EAC2PP
3057		FMT_SMR.1 Security roles fulfilled by
3058		FMT_SMR.1/PACE_EAC2PP

- 3059 FMT\_MTD.1.1/Resume\_PIN\_EAC2PP
- 3060 The TSF shall restrict the ability to  $\underline{resume}^{245}$  the <u>suspended PIN</u><sup>246</sup> to <u>the Electronic</u> 3061 Document Holder<sup>247</sup>
- 3062 97. Application note (taken from [6], application note 42)

Resuming is a two-step procedure, subsequently using PACE with the CAN and PACE with the PIN. It must be implemented according to [17], and is relevant for the status as required by FIA\_AFL.1/Suspend\_PIN\_EAC2PP. The Electronic Document Holder is authenticated as required by FIA\_UAU.1/PACE\_EAC2PP using the PIN as the shared password.

- 3067 FMT\_MTD.1/Unblock\_PIN\_EAC2PP3068 Management of TSF data Unblocking PIN
- 3069 Hierarchical to: No other components 3070 **Dependencies:** FMT\_SMF.1 Specification of management functions fulfilled by FMT\_SMF.1/EAC2PP 3071 3072 FMT SMR.1 Security roles fulfilled by 3073 FMT\_SMR.1/PACE\_EAC2PP
- 3074 FMT\_MTD.1.1/Unblock\_PIN\_EAC2PP

<sup>&</sup>lt;sup>243</sup> [assignment: the authorized identified roles]

<sup>&</sup>lt;sup>244</sup> [assignment: the authorised identified roles that match the list of PIN changing rules conformant to [17]]

<sup>&</sup>lt;sup>245</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>246</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>247</sup> [assignment: the authorized identified roles]



- 3075 The TSF shall restrict the ability to <u>unblock</u><sup>248</sup> the <u>blocked PIN</u><sup>249</sup> to
- 3076 1. the Electronic Document Holder (using the PUK for unblocking),
- 3077
   2. <u>an EAC2 terminal of a type that has the terminal authorization level for PIN</u>
   3078 management.<sup>250</sup>
- 3079 98. Application note (taken from [6], application note 43)

The unblocking procedure must be implemented according to [17], and is relevant for the status as required by FIA\_AFL.1/Block\_PIN\_EAC2PP. It can be triggered by either (i) the Electronic Document Holder being authenticated as required by FIA\_UAU.1/PACE\_EAC2PP using the PUK as the shared password or (ii) an EAC2 terminal (FIA\_UAU.1/EAC2\_Terminal\_EAC2PP) that proved a terminal authorization level being sufficient for PIN management (FDP\_ACF.1/TRM).

# 3086 FMT\_MTD.1/Activate\_PIN\_EAC2PP3087 Management of TSF data – Activating/Deactivating PIN

- Management of 15F data Activating/Deactivating Pin
- 3089 Dependencies:FMT\_SMF.1 Specification of management functions3090fulfilled by FMT\_SMF.1/EAC2PP3091FMT\_SMR.1 Security roles fulfilled by

No other components

- 3092 FMT\_SMR.1/PACE\_EAC2PP
  - 3093 FMT\_MTD.1.1/Activate\_PIN\_EAC2PP
  - 3094 The TSF shall restrict the ability to <u>activate and deactivate<sup>251</sup></u> the <u>PIN<sup>252</sup></u> to <u>an EAC2</u> 3095 terminal of a type that has the terminal authorization level for PIN management<sup>253</sup>.
  - 3096 99. Application note (taken from [6], application note 44)

The activation/deactivation procedures must be implemented according to [17]. They can be triggered by an EAC2 terminal (FIA\_UAU.1/EAC2\_Terminal\_EAC2PP) that proved a terminal authorization level sufficient for PIN management (FDP\_ACF.1/TRM).

3100 FMT\_MTD.3/EAC2PP

Hierarchical to:

**3101** Secure TSF data

3088

3102 Hierarchical to:

No other components

<sup>&</sup>lt;sup>248</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>249</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>250</sup> [assignment: the authorized identified roles]

<sup>&</sup>lt;sup>251</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>252</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>253</sup> [assignment: *the authorized identified roles*]



3103	Dependencies:	FMT_MTD.1 Management of TSF data fulfilled by
3104		FMT_MTD.1/CVCA_INI_EAC2PP,
3105		FMT_MTD.1/CVCA_UPD_EAC2PP,
3106		FMT_MTD.1/DATE_EAC2PP

- 3107 FMT\_MTD.3.1\_EAC2PP
- 3108 The TSF shall ensure that only secure values of the certificate chain are accepted for
- 3109 TSF data of the Terminal Authentication protocol 2 and the Access Control SFP<sup>254</sup>.
- 3110 **Refinement: To determine if the certificate chain is valid, the TOE shall proceed the**
- 3111 certificate validation according to [18].
- 3112 100. Application note (taken from [6], application note 45)

Terminal Authentication is used as required by (i) FIA\_UID.1/EAC2\_Terminal\_EAC2PP and FIA\_UAU.5/PACE\_EAC2PP. The terminal authorization level derived from the CVCA Certificate, the DV Certificate and the Terminal Certificate is used as TSF-data for the access control required by FDP\_ACF.1/TRM.

- 3117 In addition, this ST contains all remaining SFRs of the claimed [13].
- 3118 FMT\_LIM.1/EAC2PP
- 3119 Limited capabilities
- 3120 Hierarchical to: No other components
- 3121 Dependencies:FMT\_LIM.2Limitedavailability:fulfilledby3122FMT\_LIM.2/EAC2PP
- 3123 FMT\_LIM.1.1\_EAC2PP

3128

- 3124 The TSF shall be designed in a manner that limits their capabilities so that in conjunction
- 3125 with 'Limited availability (FMT\_LIM.2)' the following policy is enforced:
- 3126 Deploying test features after TOE delivery do not allow
- 3127 1. User Data to be manipulated and disclosed,
  - 2. <u>TSF data to be manipulated or disclosed.</u>
- 3129 3. software to be reconstructed,
- 3130
   4. <u>substantial information about construction of TSF to be gathered which may enable</u>
   3131
   <u>other attacks.<sup>255</sup> and</u>

<sup>&</sup>lt;sup>254</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>255</sup> [assignment: Limited capability and availability policy]



3132	5. EAC1 and EAC2 pro	tected data <sup>256</sup>	
3133	Application note 101 (from ST author)		
3134	The assignment was necessary to cover all protected user data.		
3135 3136	FMT_LIM.2/EAC2PP Limited availability		
3137	Hierarchical to:	No other components	
3138	Dependencies:	FMT_LIM.1 Limited capabilities: fulfilled by	
3139		FMT_LIM.1/EAC2PP	
3140	FMT_LIM.2.1_EAC2PP		
3141	The TSF shall be designed in a manner that limits their availability so that in conjunctio		
3142	with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced:		
3143	Deploying test features after TOE delivery do not allow		
3144	1. User Data to be man	ipulated and disclosed,	
3145	2. TSF data to be manip	pulated or disclosed.	
3146	3. software to be recons	structed,	
3147	4. substantial information	n about construction of TSF to be gathered which may enable	
3148	other attacks.257 and		
3149	5. EAC1 and EAC2 pro-	tected data <sup>258</sup>	
3150	Application note 102 (from ST author)		
3151	The assignment was necessary to cover all protected user data.		
3152 3153	FMT_MTD.1/INI_ENA_EAC2PP Management of TSF data – Writing Initialisation and Pre-personalisation Data		
3154	Hierarchical to:	No other components	
3155	Dependencies:	FMT_SMF.1 Specification of management functions:	
3156		fulfilled by FMT_SMF.1/EAC2PP	

 <sup>&</sup>lt;sup>256</sup> [assignment: Limited capability and availability policy]
 <sup>257</sup> [assignment: Limited capability and availability policy]
 <sup>258</sup> [assignment: Limited capability and availability policy]


IDentity Applet v3.4/eIDAS Security Target

3157 3158		FMT_SMR.1 FMT_SMR.1/PA		roles:	fulfilled	by
3159	FMT_MTD.1.1/INI_ENA_EAC2PP					
3160 3161	The TSF shall restrict the ability <u>Data<sup>260</sup> to the Manufacturer</u> . <sup>261</sup>	/ to <u>write<sup>259</sup> the Initi</u>	alisation Da	ta and Pre	-personalisa	<u>ation</u>
3162 3163	FMT_MTD.1/INI_DIS_EAC2PP Management of TSF data – Reading an	nd Using Initialisatio	on and Pre-p	ersonalisat	tion Data	
3164	Hierarchical to:	No other compon	nents			
3165 3166	Dependencies:	FMT_SMF.1 Spe fulfilled by FMT_S		•	ment functi	ons:
3167		FMT_SMR.1	Security	roles:	fulfilled	by
3168		FMT_SMR.1/PAG	CE_EAC2PI	D		
3169	FMT_MTD.1.1/INI_DIS_EAC2PP					
3170	The TSF shall restrict the ab	ility to <u>read out<sup>262</sup></u>	the Initialis	sation Dat	a and the	Pre-
3171	personalisation Data <sup>263</sup> to the P	ersonalisation Ager	<u>nt</u> . <sup>264</sup>			
3172	The following SFRs are imported d	ue to claiming [5].	They mainly	concern a	applications	with
3173	EAC1-protected data.					
3174	• FMT_SMF.1/EAC1PP					
3175	• FMT_SMR.1/PACE_EAC1P	Р				
3176	This SFR is combined with FMT_SM	/R.1/PACE_EAC2F	PP into <b>FMT</b>	_ <b>SMR.1</b> .		
3177	• FMT_LIM.1/EAC1PP					

3178 This SFR is equivalent to **FMT\_LIM.1/EAC2PP**, but listed here for the sake of completeness.

<sup>&</sup>lt;sup>259</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>260</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>261</sup> [assignment: *the authorised identified roles*]

<sup>&</sup>lt;sup>262</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>263</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>264</sup> [assignment: *the authorized identified roles*]

#### 3179 • FMT\_LIM.2/EAC1PP

- 3180 This SFR is equivalent to **FMT\_LIM.2/EAC2PP**, but listed here for the sake of completeness.
- 3181 FMT\_MTD.1/INI\_ENA\_EAC1PP
- 3182 (equivalent to **FMT\_MTD.1/INI\_ENA\_EAC2PP**, but listed here for the sake of completeness)
- 3183 FMT\_MTD.1/INI\_DIS\_EAC1PP
- 3184 (equivalent to FMT\_MTD.1/INI\_DIS\_EAC2PP, but listed here for the sake of completeness)
- 3185 FMT\_MTD.1/CVCA\_INI\_EAC1PP
- 3186 FMT\_MTD.1/CVCA\_UPD\_EAC1PP
- 3187 FMT\_MTD.1/DATE\_EAC1PP

3188 This SFR is equivalent to **FMT\_MTD.1/DATE\_EAC2PP**. Note that 3189 FMT\_MTD.1/DATE\_EAC2PP generalizes the notion of Domestic Extended Inspection System 3190 to EAC1 terminals with appropriate authorization level. This does not violate strict conformance 3191 to [5].

- 3192 FMT\_MTD.1/CAPK\_EAC1PP
- 3193 FMT\_MTD.1/PA\_EAC1PP
- 3194 FMT\_MTD.1/KEY\_READ\_EAC1PP
- 3195 FMT\_MTD.3/EAC1PP
- 3196 FMT\_SMF.1/EAC1PP
- **3197** Specification of Management Functions
- 3198 Hierarchical to: No other components
- 3199 Dependencies: No dependencies
- 3200 FMT\_SMF.1.1/EAC1PP
- 3201 The TSF shall be capable of performing the following management functions:
- 3202 1. <u>Initialization</u>,
- 3203 2. <u>Pre-personalisation</u>,
- 3204 3. <u>Personalisation</u>

3205	4. <u>Configuration.</u> <sup>265</sup>	
3206 3207	FMT_MTD.1/CVCA_INI_EAC1PP Management of TSF data – Initializati	on of CVCA Certificate and Current Date
3208	Hierarchical to:	No other components
3209 3210	Dependencies:	FMT_SMF.1 Specification of management functions fulfilled by FMT_SMF.1/EAC1PP
3211		FMT_SMR.1 Security roles fulfilled by
3212		FMT_SMR.1/PACE_EAC1PP
3213	FMT_MTD.1.1/CVCA_INI_EAC1PP	
3214	The TSF shall restrict the ability	v to <u>write</u> <sup>266</sup> the
3215	1. initial Country Verifying (	Certification Authority Public Key,
3216	2. initial Country Verifying (	Certification Authority Certificate,
3217	3. initial Current Date,	
3218	4. <u>none</u> <sup>267268</sup>	
3219	to Personalisation Agent <sup>269</sup> .	
3220	103. Application note (taken from [5], app	blication note 41)
3221	Applied.	
3222 3223	FMT_MTD.1/CVCA_UPD_EAC1PP Management of TSF data – Country V	erifying Certification Authority
3224	Hierarchical to:	No other components
3225	Dependencies:	FMT_SMF.1 Specification of management functions
3226		functions fulfilled by FMT_SMF.1/EAC1PP
3227		FMT_SMR.1 Security roles fulfilled by
3228		FMT_SMR.1/PACE_EAC1PP

 <sup>&</sup>lt;sup>265</sup> [assignment: list of management functions to be provided by the TSF]
 <sup>266</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]
 <sup>267</sup> [assignment: list of TSF data]

<sup>&</sup>lt;sup>268</sup> [assignment: *list of TSF data*]
<sup>269</sup> [assignment: *the authorised identified roles*]

- 3229 FMT\_MTD.1.1/CVCA\_UPD\_EAC1PP
- 3230 The TSF shall restrict the ability to <u>update</u><sup>270</sup> the
- 3231 1. <u>Country Verifying Certification Authority Public Key</u>,
- 3232 2. <u>Country Verifying Certification Authority Certificate<sup>271</sup></u>
- 3233 to <u>Country Verifying Certification Authority</u>.<sup>272</sup>
- 3234 104. Application note (taken from [5], application note 42)

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

- 3239 FMT\_MTD.1/CAPK\_EAC1PP3240 Management of TSF data Chip Authentication Private Key
- 3241 Hierarchical to: No other components
- 3242Dependencies:FMT\_SMF.1Specification of management functions3243functions fulfilled by FMT\_SMF.1/EAC1PP
- 3244FMT\_SMR.1Securityrolesfulfilledby3245FMT\_SMR.1/PACE\_EAC1PP
- 3246 FMT\_MTD.1.1/CAPK\_EAC1PP
- 3247 The TSF shall restrict the ability to <u>create, load</u><sup>273274</sup> the <u>Chip Authentication Private Key</u><sup>275</sup>
- 3248 to Manufacturer or Personalisation Agent.<sup>276</sup>
- 3249 105. Application note (taken from [5], application note 44)
- 3250 Applied.
- 3251 FMT\_MTD.1/PA\_EAC1PP
- 3252 Management of TSF data Personalisation Agent

<sup>&</sup>lt;sup>270</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>271</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>272</sup> [assignment: the authorised identified roles]

<sup>&</sup>lt;sup>273</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>274</sup> [selection: create, load]

<sup>&</sup>lt;sup>275</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>276</sup> [assignment: the authorisedidentified roles]



3253	Hierarchical to:	No other components
3254 3255	Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1/EAC1PP
3256 3257		FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE_EAC1PP
3258	FMT_MTD.1.1/PA_EAC1PP	
3259 3260	The TSF shall restrict the ability Personalisation Agent. <sup>279</sup>	to write <sup>277</sup> the Document Security Object $(SO_D)^{278}$ to the
3261 3262	FMT_MTD.1/KEY_READ_EAC1PP Management of TSF data – Key Read	
3263	Hierarchical to:	No other components
3264 3265	Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1/EAC1PP
3266 3267 3268		FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/PACE_EAC1PPFMT_MTD.1.1/KEY_RE AD_EAC1PP
3269		
	The TSF shall restrict the ability	to <u>read</u> <sup>280</sup> the
3270	1. <u>PACE passwords,</u>	to <u>read</u> <sup>280</sup> the
3270 3271		
	1. PACE passwords,	ate Key.
3271	<ol> <li><u>PACE passwords,</u></li> <li><u>Chip Authentication Priva</u></li> </ol>	ate Key. 295 <sup>281</sup>

3275 106. Application note (taken from [5], application note 45)

<sup>&</sup>lt;sup>277</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

 <sup>&</sup>lt;sup>278</sup> [assignment: *list of TSF data*]
 <sup>279</sup> [assignment: *the authorised identified roles*]

<sup>&</sup>lt;sup>280</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>281</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>282</sup> [assignment: the authorised identified roles]



- The SFR FMT\_MTD.1/KEY\_READ\_EAC1PP in the ST covers the definition in [13] and 3276 3277 extends it by additional TSF data. This extension does not conflict with the strict conformance 3278 to [13].
- 3279 **107.** Application note (ST author)
- 3280 The refinement was necessary because of the Active Authentication protocol.
- 3281 FMT\_MTD.3/EAC1PP 3282
- Secure TSF data
- Hierarchical to: 3283 No other components
- FMT\_MTD.1 Management of TSF data fulfilled by 3284 Dependencies: FMT\_MTD.1/CVCA\_INI\_EAC1PP 3285 and 3286 FMT\_MTD.1/CVCA\_UPD\_EAC1PP
- 3287 FMT MTD.3.1 EAC1PP
- 3288 The TSF shall ensure that only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol v.1 and the Access Control.<sup>283</sup> 3289
- 3290 Refinement: The certificate chain is valid if and only if
- 3291 1. the digital signature of the Inspection System Certificate can be verified as 3292 correct with the public key of the Document Verifier Certificate and the 3293 expiration date of the Inspection System Certificate is not before the Current 3294 Date of the TOE.
- 3295 2. the digital signature of the Document Verifier Certificate can be verified as 3296 correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Certificate of the Country 3297 3298 Verifying Certification Authority is not before the Current Date of the TOE and 3299 the expiration date of the Document Verifier Certificate is not before the Current 3300 Date of the TOE.
- 3. the digital signature of the Certificate of the Country Verifying Certification 3301 3302 Authority can be verified as correct with the public key of the Country Verifying 3303 Certification Authority known to the TOE.

<sup>&</sup>lt;sup>283</sup> [assignment: *list of TSF data*]



- 3304The Inspection System Public Key contained in the Inspection System Certificate in3305a valid certificate chain is a secure value for the authentication reference data of the3306Extended Inspection System EAC1 terminal.
- 3307 The intersection of the Certificate Holder Authorizations contained in the
- 3308 certificates of a valid certificate chain is a secure value for Terminal Authorization
- 3309 of a successful authenticated Extended Inspection System EAC1 terminal.
- 3310 108. Application note (taken from [5], application note 46)

The Terminal Authentication Version 1 is used for EAC1 terminal as required by FIA\_UAU.4/PACE\_EAC1PP and FIA\_UAU.5/PACE\_EAC1PP. The Terminal Authorization is used as TSF data for access control required by FDP\_ACF.1/TRM.

- The following SFRs are imported due to claiming [14]. They mostly concern the security management of an *eSign* application.
- FMT SMR.1/SSCDPP
- **• FMT\_SMF.1/SSCDPP**
- 3318 FMT\_MOF.1/SSCDPP
- 3319 FMT\_MSA.1/Admin\_SSCDPP
- 3320 FMT\_MSA.1/SignatorySSCDPP
- 3321 FMT\_MSA.2/SSCDPP
- 3322 FMT\_MSA.3/SSCDPP
- 3323 FMT\_MSA.4/SSCDPP
- FMT\_MTD.1/Admin\_SSCDPP
- **FMT\_MTD.1/Signatory\_SSCDPP**
- 3326 FMT\_SMR.1/SSCDPP
- 3327 Security roles
- 3328 Hierarchical to: No other components
- 3329Dependencies:FIA\_UID.1Timing of identification fulfilled by3330FIA\_UID.1/SSCDPP
- 3331 FMT\_SMR.1.1/SSCDPP
- 3332 The TSF shall maintain the roles <u>R.Admin and R.Sigy<sup>284</sup></u>

<sup>&</sup>lt;sup>284</sup> [assignment: the authorised identified roles]

3333	FMT_SMR.1.2/SSCDPP			
3334	The TSF shall be able to associate users with roles.			
3335 3336	FMT_SMF.1/SSCDPP Security Management Functions			
3337	Hierarchical to:	No other components		
3338	Dependencies:	No dependencies		
3339	FMT_SMF.1.1/SSCDPP			
3340	The TSF shall be capable of per	forming the following management functions:		
3341	1. Creation and modification	n of RAD,		
3342	2. Enabling the signature cr	eation function,		
3343	3. Modification of the securi	ty attribute SCD/SVD management, SCD operational,		
3344		of the security attribute SCD Identifier, <sup>285</sup>		
3345	5. <u>Unblock the RAD</u> <sup>286</sup>			
3346	109. Application note (taken from [14], ap	olication note 14)		
3347	Applied.			
3348 3349	FMT_MOF.1/SSCDPP Management of security functions beh	aviour		
3350	Hierarchical to:	No other components		
3351	Dependencies:	FMT_SMR.1 Security roles fulfilled by		
3352		FMT_SMR.1/SSCDPP		
3353		FMT_SMF.1 Specification of Management Functions		
3354		fulfilled by FMT_SMF.1/SSCDPP		
3355	FMT_MOF.1.1/SSCDPP			
3356	The TSF shall restrict the ability	to enable <sup>287</sup> the functions signature creation function <sup>288</sup> to		
3357	<u>R.Sigy</u> <sup>289</sup> .			

 <sup>&</sup>lt;sup>285</sup> [assignment: list of other security management functions to be provided by the TSF]
 <sup>286</sup> [assignment: list of other security management functions to be provided by the TSF]
 <sup>287</sup> [selection: determine the behaviour of, disable, enable, modify the behaviour of]

<sup>&</sup>lt;sup>288</sup> [assignment: *list of functions*]

<sup>&</sup>lt;sup>289</sup> [assignment: the authorised identified roles]

3358 3359	FMT_MSA.1/Admin_SSCDPP Management Security attributes	
3360	Hierarchical to:	No other components
3361 3362 3363	Dependencies:	[FDP_ACC.1 Subset access control or FDP.IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/SCD/SVD_Generation_SSCDPP
3364 3365		FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/SSCDPP
3366 3367		FMT_SMF.1 Specification of Management Functions fulfilled by FMT_SMF.1/SSCDPP
3368	FMT_MSA.1.1/Admin_SSCDPP	
3369	The TSF shall enforce the SCE	O/SVD Generation SFP <sup>290</sup> to restrict the ability to modify,
3370	none <sup>291</sup> the security attributes S	CD/SVD management <sup>292</sup> to <u>R.Admin<sup>293</sup>.</u>
3371 3372	FMT_MSA.1/SignatorySSCDPP Management Security attributes	
3373	Hierarchical to:	No other components
3374 3375 3376	Dependencies:	[FDP_ACC.1 Subset access control or FDP.IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/Signature-creation_SSCDPP
3377 3378		FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/SSCDPP
3379 3380		FMT_SMF.1 Specification of Management Functions fulfilled by FMT_SMF.1/SSCDPP

FMT\_MSA.1.1/Signatory\_SSCDPP 3381

 $<sup>^{290}</sup>$  [assignment: access control SFP(s), information flow control SFP(s)]

 <sup>&</sup>lt;sup>291</sup> [assignment: *list of security attributes*]
 <sup>293</sup> [assignment: *list of security attributes*]
 <sup>293</sup> [assignment: *the authorized identified roles*]



or

and



- The TSF shall enforce the SCD/SVD Generation SFP<sup>294</sup> to restrict the ability to modify<sup>295</sup> 3382 the security attributes SCD operational<sup>296</sup> to R.Sigy<sup>297</sup>. 3383
- 3384 FMT\_MSA.2/SSCDPP
- 3385 Secure security attributes
- 3386 Hierarchical to: No other components 3387 Dependencies: [FDP ACC.1 Subset control access 3388 FDP.IFC.1 Subset information flow control] fulfilled by 3389 FDP ACC.1/SCD/SVD Generation SSCDPP FDP\_ACC.1/Signature-creation\_SSCDPP 3390
- 3391 FMT\_MSA.1 Management of security attributes fulfilled FMT MSA.1/Admin SSCDPP 3392 by and 3393 FMT MSA.1/SignatorySSCDPP.
- 3394 fulfilled FMT SMR.1 Security roles by 3395 FMT\_SMR.1/SSCDPP
- 3396 FMT\_MSA.2.1/ SSCDPP
- 3397 The TSF shall ensure that only secure values are accepted for SCD/SVD Management and SCD operational<sup>298</sup>. 3398
- 3399 110. Application note (taken from [14], application note 15)
- 3400 Applied.
- 3401 FMT\_MSA.3/SSCDPP
- 3402 Static attribute initialisation

3403	Hierarchical to:	No other c	omponents	
3404	Dependencies:	FMT_MSA	1.1 Management of security attributes ful	filled
3405		by	FMT_MSA.1/Admin_SSCDPP	and
3406		FMT_MSA	.1/SignatorySSCDPP.	

<sup>&</sup>lt;sup>294</sup> [assignment: access control SFP(s), information flow control SFP(s)]

<sup>&</sup>lt;sup>295</sup> [selection: change\_default, query, modify, delete, [assignment: other operations]]

<sup>&</sup>lt;sup>296</sup> [assignment: *list of security attributes*]

<sup>&</sup>lt;sup>297</sup> [assignment: the authorized identified roles]

<sup>&</sup>lt;sup>298</sup> [selection: *list of security attributes*]



3407 3408		IT_SMR.1 Security roles fulfilled by IT_SMR.1/SSCDPP
3409	FMT_MSA.3.1/ SSCDPP	
3410	The TSF shall enforce the <u>SCD/SVD</u>	OGeneration SFP, SVD Transfer SFP and Signature
3411	Creation SFP <sup>299</sup> to provide restrictive	<sup>300</sup> default values for security attributes that are used
3412	to enforce SFP.	
3413	FMT_MSA.3.2/ SSCDPP	
3414	The TSF shall allow the <u>R.Admin</u> <sup>30</sup>	<sup>1</sup> to specify alternative initial values to override the
3415	default values when an object or info	rmation created.
3416 3417	FMT_MSA.4/SSCDPP Security attribute value inharitance	
3418	Hierarchical to: No	other components
3419 3420		DP_ACC.1 Subset access control or P.IFC.1 Subset information flow control] fulfilled by
3421	FD	P_ACC.1/SCD/SVD_Generation_SSCDPP and
3422	FD	P_ACC.1/Signature-creation_SSCDPP
3423	FMT_MSA.4/SSCDPP	
3424	The TSF shall use the following rules	s to set the value of security attributes:
3425	1. If S.Admin successfully ge	nerates an SCD/SVD pair without S.Sigy being
3426	authenticated the security att	tribute "SCD operational of the SCD" shall be set to
3427	"no" as a single operation.	
3428	2. If S.Sigy successfully generation	ates an SCD/SVD pair the security attribute "SCD
3429	operational of the SCD" shall	be set to "yes" as a single operation. 302

- 3430 111. Application note (taken from [14], application note 16)
- The TOE may not support generating an SVD/SCD pair by the signatory alone, in which case rule (2) is not relevant.

<sup>&</sup>lt;sup>299</sup> [assignment: access control SFP, information flow control SFP]

<sup>&</sup>lt;sup>300</sup> [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

<sup>&</sup>lt;sup>301</sup> [assignment: *the authorised identified roles*]

<sup>&</sup>lt;sup>302</sup> [assignment: rules for setting the values of security attributes]

3433 3434	FMT_MTD.1/Admin_SSCDPP Management of TSF data	
3435	Hierarchical to:	No other components
3436 3437	Dependencies:	FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/SSCDPP
3438 3439		FMT_SMF.1 Specification of Management Functions fulfilled by FMT_SMF.1/SSCDPP
3440	FMT_MTD.1.1/Admin_SSCDPP	
3441	The TSF shall restrict the ability	to create <sup>303</sup> the RAD <sup>304</sup> to R.Admin <sup>305</sup> .
3442 3443	FMT_MTD.1/Signatory_SSCDPP Management of TSF data	
3444	Hierarchical to:	No other components
3445 3446	Dependencies:	FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/SSCDPP
3447 3448		FMT_SMF.1 Specification of Management Functions fulfilled by FMT_SMF.1/SSCDPP
3449	FMT_MTD.1.1/Signatory_SSCDPP	
3450	The TSF shall restrict the ability	to modify <sup>306</sup> , <u>none</u> <sup>307</sup> the <u>RAD</u> <sup>308</sup> to <u>R.Sigy</u> <sup>309</sup> .
3451	112. Application note (taken from [14], ap	pplication note 17)
3452	Applied.	
3453 3454	The following SFRs are defined he manufacturing and relate directly to	re. The concern loading applications onto the IC during

- 3454 manufacturing and relate directly to OT.Cap\_Avail\_Loader.
- 3455 FMT\_LIM.1/Loader
- 3456 Limited Capabilities

<sup>304</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>303</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]

<sup>&</sup>lt;sup>305</sup> [assignment: the authorised identified roles]

<sup>&</sup>lt;sup>306</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]

<sup>&</sup>lt;sup>307</sup> [selection: change\_default, query, modify, delete, clear, [assignment: other operations]

<sup>&</sup>lt;sup>308</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>309</sup> [assignment: *the authorised identified roles*]



3457	Hierarchical to:	No othe	er compoi	nents			
3458 3459	Dependencies:	FMT_ FMT_L	LIM.2 IM.2/Load		availability	fulfilled	by

- 3460 FMT\_LIM.1.1/Loader
- 3461 The TSF shall be designed and implemented in a manner that limits their capabilities so
- 3462 that in conjunction with "Limited availability (FMT\_LIM.2)" the following policy is enforced:
- 3463 Deploying Loader functionality after the locking of the Loader<sup>310</sup> does not allow stored user
- 3464 data to be disclosed or manipulated by unauthorized users.<sup>311</sup>
- 3465 113. Application note (taken from [20], application note 14)

FMT\_LIM.1/Loader supplements FMT\_LIM.2/Loader allowing for non-overlapping loading of
 user data and protecting the TSF against misuses of the Loader for attacks against the TSF.
 The TOE Loader may allow for correction of already loaded user data before the assigned
 action e.g. before blocking the TOE Loader for TOE Delivery to the end-customer or any
 intermediate step on the life cycle of the Security IC or the smartcard.

- 3471 FMT\_LIM.2/Loader
- 3472 Limited Availability
- 3473 Hierarchical to: No other components
- 3474 Dependencies:FMT\_ LIM.1 Limited capabilities fulfilled by3475FMT\_LIM.1/Loader
- 3476 FMT\_LIM.2.1/Loader
- 3477 The TSF shall be designed and implemented in a manner that limits their availability so
- 3478 that in conjunction with "Limited capabilities (FMT\_LIM.1)" the following policy is enforced:
- 3479 The TSF prevents deploying the Loader functionality after the locking of the Loader.<sup>312313</sup>
- 3480 114. Application note (taken from [20], application note 15)

The Loader functionality relies on a secure boot loading procedure in a secure environment before TOE delivery to the assigned user and preventing to deploy the Loader of the Security IC after an assigned action, e.g. after blocking the Loader for TOE delivery to the end-user.

3484 The following SFR is new and concern security management for ePassport application in 3485 combination with [5] in case the Active Authentication protocol is active:

<sup>&</sup>lt;sup>310</sup> [assignment: *action*]

<sup>&</sup>lt;sup>311</sup> [assignment: *Limited capability and availability policy*]

<sup>&</sup>lt;sup>312</sup> [assignment: *action*]

<sup>&</sup>lt;sup>313</sup> [assignment: *Limited capability and availability policy*]



3486	FMT_MTD.1/AA_Private_Key
3487	Management of TSF data – Active Authentication Private Key

3488	Hierarchical to:	No other components	
3489 3490	Dependencies:	FMT_SMF.1 Specification of management functions fulfilled by FMT_SMF.1/EAC1PP	
3491		FMT_SMR.1 Security roles fulfilled by	
3492		FMT_SMR.1/PACE_EAC1PP	

- 3493 FMT\_MTD.1.1/AA\_Private\_Key
- 3494 The TSF shall restrict the ability to <u>create or load</u><sup>314</sup> the <u>Active Authentication Private</u> 3495 <u>Key</u><sup>315</sup> to <u>the Personalization Agent</u>.<sup>316</sup>
- 3496 **6.1.7. Class FPT**
- 3497 The following security functional requirements are imported from [6], and address the 3498 protection against forced illicit information leakage, including physical manipulation.

#### 3499 • FPT\_EMS.1/EAC2PP

- 3500 115. Application note (taken from [20], application note 16)
- Note that related to Application Note 6 of [20], the PIN in the above SFR refers here to both the PIN for an eID application, and also the PIN for an eSign application, if they exist on card.
- 3503 FPT\_FLS.1/EAC2PP
- **FPT\_TST.1/EAC2PP**
- 3505 FPT\_PHP.3/EAC2PP
- The following SFRs are imported due to claiming [5]. They mostly concern the protection of security functionality related to EAC1-protected data.

#### 3508 • **FPT\_TST.1/EAC1PP**

3509 (equivalent to **FPT\_TST.1/EAC2PP**, but listed here for the sake of completeness)

<sup>&</sup>lt;sup>314</sup> [assignment: change\_default, query, modify, delete, clear, [assignment: other operations]]

<sup>&</sup>lt;sup>315</sup> [assignment: *list of TSF data*]

<sup>&</sup>lt;sup>316</sup> [assignment: the authorized identified roles]

#### 3510 • FPT\_FLS.1/EAC1PP

3511 (equivalent to **FPT\_FLS.1/EAC2PP**, but listed here for the sake of completeness)

#### 3512 • FPT\_PHP.3/EAC1PP

3513 (equivalent to **FPT\_PHP.3/EAC2PP**, but listed here for the sake of completeness)

#### **• FPT\_EMS.1/EAC1PP**

The following SFRs are imported due to claiming [14]. They mostly concern the protection of security functionality related to eSign application (if available).

- 3517 FPT\_EMS.1/SSCDPP
- 3518 FPT\_FLS.1/SSCDPP
- 3519 (subsumed by **FPT\_FLS.1/EAC2PP**)
- 3520 **FPT\_PHP.1/SSCDPP**
- 3521 FPT\_PHP.3/SSCDPP
- 3522 (subsumed by **FPT\_PHP.3/EAC2PP**)
- 3523 FPT\_TST.1/SSCDPP
- 3524 (subsumed by **FPT\_TST.1/EAC2PP**)
- 3525 FPT\_EMS.1/EAC2PP3526 TOE Emanation
- 3527 Hierarchical to: No other components
- 3528 Dependencies: No dependencies
- 3529 FPT\_EMS.1.1/EAC2PP
- 3530 The TOE shall not emit <u>variations in power consumption or timing during command</u>
- 3531 <u>execution<sup>317</sup> in excess of non-useful information<sup>318</sup> enabling access to</u>
- 3532 1. the session keys (PACE-K<sub>MAC</sub>, PACE-K<sub>Enc</sub>), (CA-K<sub>MAC</sub>, CA-K<sub>Enc</sub>),

<sup>&</sup>lt;sup>317</sup> [assignment: types of emissions]

<sup>&</sup>lt;sup>318</sup> [assignment: *specified limits*]

3533	2.	the ephemeral private key ephem-SK <sub>PICC</sub> -PACE, 319
3534	3.	the Chip Authentication private keys (SKPICC)
3535	4.	the PIN, PUK,
3536	5.	<u>none</u> <sup>320</sup>
3537	and	
3538	6.	the Restricted Identification private key(s) SKID, 321
3539	7.	none. <sup>322</sup>
3540	FPT_EMS	1.2/EAC2PP
3541	The T	SF shall ensure any users <sup>323</sup> are unable to use the following interface electronic
3542	<u>docun</u>	nent's contactless/contact-based interface and circuit contacts <sup>324</sup> to gain access to
3543	1.	the session keys (PACE-K <sub>MAC</sub> , PACE-K <sub>Enc</sub> ), <b>(CA2-K<sub>MAC</sub>, CA2-K<sub>Enc</sub>),</b>
3544	2.	the ephemeral private key ephem -SK <sub>PICC</sub> -PACE1,
3545	3.	the Chip Authentication private key(s) (SK <sub>PICC</sub> ),
3546	4.	the PIN, PUK,
3547	5.	<u>the session keys (PACE-K<sub>MAC</sub>, PACE-K<sub>Enc</sub>), (CA-K<sub>MAC</sub>, CA-K<sub>Enc</sub>)<sup>325</sup></u>
3548	6.	none <sup>326</sup>
3549	and	
3550	7.	the Restricted Identification private key(s) $SK_{ID_4}^{327}$
3551	8.	<u>none</u> . <sup>328</sup>

3552 116. Application note (taken from [6], application note 46)

The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE, originate from internal operation of the TOE, or be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. Examples of measurable phenomena include, but are not limited to variations in power

<sup>&</sup>lt;sup>319</sup> [assignment: *list of types of TSF data* ]

<sup>&</sup>lt;sup>320</sup> [assignment: *list of types of TSF data*]

<sup>&</sup>lt;sup>321</sup> [assignment: *list of types of user data* ]

<sup>&</sup>lt;sup>322</sup> [assignment: *list of types of user data*]

<sup>&</sup>lt;sup>323</sup> [assignment: *type of users*]

<sup>&</sup>lt;sup>324</sup> [assignment: *type of connection*]

<sup>&</sup>lt;sup>325</sup> [assignment: *list of types of TSF data*]

<sup>&</sup>lt;sup>326</sup> [assignment: *list of types of TSF data*]

<sup>&</sup>lt;sup>327</sup> [assignment: *list of types of user data*]

<sup>&</sup>lt;sup>328</sup> [assignment: *list of types of user data*]



3559 consumption, timing of signals, and electromagnetic radiation due to internal operations or 3560 data transmissions.

Note that while the security functionality described in FPT\_EMS.1/EAC2PP should be taken into account during development of the TOE, associated tests must be carried out as part of the evaluation, and not/not only during product development.

- Note that in the above SFR, all items in FPT\_EMS.1/EAC2PP from 3. upwards are additional assignments. The first item is slightly refined to include CA-key(s).
- 3566 117. Application note (from ST author)
- The PIN in the above SFR refers here to both the PIN for an eID application, and also the PIN for an eSign application, if they exist on card.

The above SFR is refined from [6] by adding all relevant key material from Chip Authentication 2, the additional assignment to cover the private sector keys. Thus, the set of keys that need to be protected is a superset of the ones of the SFR from [6]. Hence, the requirement is stricter than the one from [6], and the refinement operation is justified.

- The FPT\_EMS.1.2/EAC2PP is refined because in the [20] first and fifth point is identical and unnecessary to repeat the first point in the current ST.
- 3575 FPT\_FLS.1/EAC2PP3576 Failure with preservation of secure state
- 3577 Hierarchical to: No other components
- 3578 Dependencies: No dependencies
- 3579 FPT\_FLS.1.1\_EAC2PP
- 3580 The TSF shall preserve a secure state when the following types of failures occur:
- 3581 1. Exposure to operating conditions causing a TOE malfunction,
  - 2. Failure detected by TSF according to FPT\_TST.1,<sup>329</sup>
- 3583 3. <u>none</u>.<sup>330</sup>
- 3584 FPT\_TST.1/EAC2PP
- 3585 TSF testing

3582

- 3586 Hierarchical to: No other components
- 3587 Dependencies: No dependencies
- 3588 FPT\_TST.1.1/EAC2PP

<sup>&</sup>lt;sup>329</sup> [assignment: *list of types of failures in the TSF*]

<sup>&</sup>lt;sup>330</sup> [assignment: list of types of failures in the TSF]



- 3589 The TSF shall run a suite of self tests during <u>initial start-up</u>, <u>periodically during normal</u> 3590 <u>operation</u><sup>331</sup>to demonstrate the correct operation of <u>the TSF</u>.<sup>332</sup>
- 3591 FPT\_TST.1.2/EAC2PP
- 3592 The TSF shall provide authorised users with the capability to verify the integrity of <u>the TSF</u> 3593 data.<sup>333</sup>
- 3594 FPT\_TST.1.3/EAC2PP
- 3595 The TSF shall provide authorised users with the capability to verify the integrity of <u>stored</u> 3596 TSF executable code.<sup>334</sup>
- **3597** FPT\_PHP.3/EAC2PP
- **3598** Resistance to physical attack
- 3599 Hierarchical to: No other components
- 3600 Dependencies:
- 3601 FPT\_PHP.3.1\_EAC2PP
- 3602 The TSF shall resist <u>physical manipulation and physical probing</u><sup>335</sup> to the <u>TSF</u><sup>336</sup> by 3603 responding automatically such that the SFRs are always enforced.

No dependencies

- 3604 FPT\_EMS.1/EAC1PP
- **3605** TOE Emanation
- 3606 Hierarchical to: No other components
- 3607 Dependencies: No dependencies
- 3608 FPT\_EMS.1.1/EAC1PP
- 3609 The TOE shall not emit variations in power consumption or timing during command
- 3610 <u>execution<sup>337</sup> in excess of non-useful information<sup>338</sup> enabling access to</u>
- 3611 1. <u>Chip Authentication (Version 1) Session Keys</u>,

<sup>&</sup>lt;sup>331</sup> [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]

<sup>&</sup>lt;sup>332</sup> [selection: [assignment: parts of TSF], the TSF]

<sup>&</sup>lt;sup>333</sup> [selection: [assignment: parts of TSF], TSF data]

<sup>&</sup>lt;sup>334</sup> [selection: [assignment: parts of TSF], TSF]

<sup>&</sup>lt;sup>335</sup> [assignment: *physical tampering scenarios*]

<sup>&</sup>lt;sup>336</sup> [assignment: *list of TSF devices/elements*]

<sup>&</sup>lt;sup>337</sup> [assignment: *types of emissions*]

<sup>&</sup>lt;sup>338</sup> [assignment: *specified limits*]

## IDentity Applet v3.4/eIDAS Security Target

PACE session Keys (PACE-K<sub>MAC</sub>, PACE-K<sub>Enc</sub>), 3612 2. 3. the ephemeral private key ephem SK<sub>PICC</sub>-PACE, 3613 the ephemeral private key SK<sub>MapPICC</sub>-PACE-CAM<sup>339</sup> 3614 4. Active Authentication Private Key<sup>340</sup> 3615 5. Personalisation Agent Key(s) 3616 6. Chip Authentication (Version 1) Private Key <sup>341</sup> and 3617 7. none 342 3618 8. 3619 FPT EMS.1.2/EAC1PP The TSF shall ensure any users<sup>343</sup> are unable to use the following interface smart card 3620 circuit contacts<sup>344</sup> to gain access to 3621 3622 1. Chip Authentication (Version 1) Session Keys, 3623 2. PACE session Keys (PACE-K<sub>MAC</sub>, PACE-K<sub>Enc</sub>), 3624 3. the ephemeral private key ephem SK<sub>PICC</sub>-PACE, 3625 4. the ephemeral private key SK<sub>MapPICC</sub>-PACE-CAM<sup>345</sup> Active Authentication Private Kev<sup>346</sup> 3626 5. 3627 Personalisation Agent Key(s) 6. Chip Authentication (Version 1) Private Key <sup>347</sup> and 7. 3628 8. none.348 3629 3630 118. Application note (from ST author) 3631 This SFR covers the definition of FPT\_EMS.1 in [5] and extends it by 4. and 5. of 3632 FPT EMS.1.1/EAC1PP and FPT EMS.1.2/EAC1PP. Also, 1. and 7. of both FPT\_EMS.1.1/EAC1PP and FPT\_EMS.1.2/EAC1PP are slightly refined in order not to confuse 3633 3634 Chip Authentication 1 with Chip Authentication 2.

3635 Note that FPT\_EMS.1/EAC1PP in [5] is solely concerned with Chip Authentication 1, but since
 3636 it was the first version of the protocol at the time, it was simply called 'Chip Authentication' back
 3637 then.

W.r.t. PACE-CAM, note the significance of protecting SK<sub>Map,PICC</sub>-PACE-CAM: Whereas when
 running PACE and CA1 separately, gaining knowledge of the ephemeral key SK<sub>PICC</sub>-PACE
 enables the attacker to decrypt the current PACE session, an attacker that gains knowledge

<sup>&</sup>lt;sup>339</sup> [assignment: *list of types of TSF data*]

<sup>&</sup>lt;sup>340</sup> [assignment: *list of types of TSF data*]

<sup>&</sup>lt;sup>341</sup> [assignment: *list of types of user data*]

<sup>&</sup>lt;sup>342</sup> [assignment: *list of types of user data*]

<sup>&</sup>lt;sup>343</sup> [assignment: *type of users*]

<sup>&</sup>lt;sup>344</sup> [assignment: *type of connection*]

<sup>&</sup>lt;sup>345</sup> [assignment: *list of types of TSF data*]

<sup>&</sup>lt;sup>346</sup> [assignment: *list of types of TSF data*]

<sup>&</sup>lt;sup>347</sup> [assignment: *list of types of TSF data*]

<sup>&</sup>lt;sup>348</sup> [assignment: *list of types of user data*]



of the ephemeral key SK<sub>Map,PICC</sub>-PACE-CAM can not only decrypt the session but also easily reveal the static secret chip authentication key SK<sub>PICC</sub>: Let ° denote the group operation (i.e. addition or multiplication), and let i(x) denote the inverse of x. Since the chip sends CA<sub>PICC</sub> = SK<sub>Map,PICC</sub>-PACE-CAM ° i(SK<sub>PICC</sub>) to the terminal, a malicious attacker that gains knowledge of SK<sub>Map,PICC</sub>-PACE-CAM can reveal SK<sub>PICC</sub> by computing SK<sub>PICC</sub> = i(CA<sub>PICC</sub>) ° SK<sub>Map,PICC</sub>-PACE-3646 CAM.

3647 Because of the Active Authentication is supported protocol by the TOE, the SFR is extended 3648 with Active Authentication Private Key.

- 3649 119. Application note (taken from[5], application note 48)
- 3650 Applied.
- 3651 FPT\_EMS.1/SSCDPP
- **3652** TOE Emanation
- 3653 Hierarchical to: No other components
- 3654 Dependencies: No dependencies
- 3655 FPT\_EMS.1.1\_SSCD
- The TOE shall not emit emit <u>variations in power consumption or timing during command</u>
   <u>execution<sup>349</sup> in excess of non-useful information<sup>350</sup> enabling access to RAD<sup>351</sup> and SCD<sup>352</sup>.</u>
- 3658 FPT\_EMS.1.2\_SSCD
- 3659 The TSF shall ensure <u>that unauthorized</u><sup>353</sup> are unable to use the following interface 3660 <u>electrical contacts</u><sup>354</sup> to gain access to RAD<sup>355</sup> and SCD<sup>356</sup>.

3661 120. Application note (taken from [14], application note 18)

The TOE shall prevent attacks against the SCD and other secret data where the attack is 3662 3663 based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or 3664 may origin by an attacker that varies the physical environment under which the TOE operates. 3665 3666 The set of measurable physical phenomena is influenced by the technology employed to 3667 implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to 3668 3669 internal operation, radio emission.

<sup>&</sup>lt;sup>349</sup> [assignment: types of emissions]

<sup>&</sup>lt;sup>350</sup> [assignment: *specified limits*]

<sup>&</sup>lt;sup>351</sup> [assignment: *list of types of TSF data*]

<sup>&</sup>lt;sup>352</sup> [assignment: *list of types of user data*]

<sup>&</sup>lt;sup>353</sup> [assignment: *type of users*]

<sup>&</sup>lt;sup>354</sup> [assignment: type of connection]

<sup>&</sup>lt;sup>355</sup> [assignment: *list of types of TSF data*]

<sup>&</sup>lt;sup>356</sup> [assignment: *list of types of user data*]



Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

- 3675 FPT\_PHP.1/SSCDPP
- **3676** Passive detection of physical attack
- 3677 Hierarchical to: No other components
- 3678 Dependencies: No dependencies
- 3679 FPT\_PHP.1.1\_SSCDPP
- 3680 The TSF shall provide unambiguous detection of physical tampering that might 3681 compromise the TSF.
- 3682 FPT\_PHP.1.2\_SSCDPP
- 3683 The TSF shall provide the capability to determine whether physical tampering with the 3684 TSF's devices or TSF's elements has occurred.
- 3685 6.2. Security Assurance Requirements for the TOE
- The assurance requirements for the evaluation of the TOE, its development and operating environment are to choose as the predefined assurance package EAL4 augmented by the following components:
- ALC\_DVS.2 (Sufficiency of security measures),
- ATE\_DPT.2 (Testing: security enforcing modules) and
- AVA\_VAN.5 (Advanced methodical vulnerability analysis).



3692 6.3.Security Requirements Rationale

## 3693 6.3.1. Security Functional Requirements Rationale

The following table provides an overview for the coverage of the security functional requirements, and also gives evidence for sufficiency and necessity of the chosen SFRs.

	OT.CA2	OT.Chip_Auth_Proof[5]	OT.Chip_Auth_Proof_PACE_CAM	OT.Chip_Auth_Proof_AA	OT.Sens_Data_Conf [5]	OT.AC_Pers_EAC2	OT.Sens_Data_EAC2	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.AC_Pers	OT.Prot_Inf_Leak	OT.RI_EAC2	OT.Non_Interfere	OT.SCD/SVD_Gen [14]	OT.Sigy_SigF ([14])	OT.Cap_Avail_Loader
Class FCS																		
FCS_CKM.1/CAM	-	-	Х	-	-	-	-	Х	Х	Х	-	-	-	-	-	-	-	-
FCS_COP.1/CAM	-	-	Х	-	-	-	-	Х	Х	Х	-	-	-	-	-	-	-	-
FCS_CKM.1/CA2	Х	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
FCS_CKM.1/RI	-	-	-	-	-	-	-	-	-	-	-	-	-	Х	-	-	-	-
FCS_CKM.1/AA	-	-	-	Х	-	-	-	-	-	-	-	-	-	-	-	-	-	-
FCS_COP.1/AA	-	-	-	Х	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Class FIA																		
FIA_UID.1/PACE_EAC1PP	-	-	Х	-	Х	-	-	Х	Х	Х	-	Х	-	-	-	-	-	-
FIA_UAU.1/PACE_EAC1PP	-	-	-	Х	Х	-	-	Х	Х	Х	-	Х	-	-	-	-	-	-
FIA_UAU.5/PACE_EAC1PP	-	-	Х	-	Х	-	-	Х	Х	Х	-	Х	-	-	-	-	-	-
FIA_API.1/PACE_CAM	-	-	Х	-	-	-	-	Х	Х	Х	-	-	-	-	-	-	-	-
FIA_UAU.1/SSCDPP	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Х	Х	



	0T.CA2	OT.Chip_Auth_Proof[5]	OT.Chip_Auth_Proof_PACE_CAM	OT.Chip_Auth_Proof_AA	OT.Sens_Data_Conf [5]	OT.AC_Pers_EAC2	OT.Sens_Data_EAC2	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.AC_Pers	OT.Prot_Inf_Leak	OT.RI_EAC2	OT.Non_Interfere	OT.SCD/SVD_Gen [14]	OT.Sigy_SigF ([14])	OT.Cap_Avail_Loader
FIA_UAU.4/PACE_EAC1PP	-	-	-	Х	-	-	-	Х	Х	Х	-	-	-	-	-	-	-	-
FIA_API.1/AA	-	-	-	Х	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Class FDP																		
FDP_ACF.1/TRM	-	-	-	-	Х	Х	Х	Х	-	Х	-	Х	-	-	Х	-	-	-
Class FMT																		
FMT_SMR.1	-	Х	-	-	-	Х	Х	Х	Х	Х	Х	Х	-	-	Х	-	-	-
FMT_LIM.1/Loader	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Х
FMT_LIM.2/Loader	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Х
FMT_MTD.1/KEY_READ_EAC1PP	-	Х	-	Х	Х	-	-	Х	Х	Х	-	Х	-	-	-	-	-	-
FMT_MTD.1/AA_Private_Key	-	-	Х		-	-	-	-	-	-	-	Х	-	-	-	-	-	-
Class FPT																		
FPT_EMS.1/EAC1PP	-	-	-	-	-	-	-	-	-	-	-	Х	Х	-	Х	-	-	-
FPT_EMS.1/EAC2PP	-	-	-	-	-	Х	-	-	-	-	-	-	Х	-	Х	-	-	-
FPT_EMS.1/SSCDPP																		

3696

Table 11 Coverage of Security Objectives for the TOE by SFRs

# 

According to [1], tracing between SFRs and security objectives must ensure that 1) each SFR
traces back to at least one security objective, and 2) that each security objective for the TOE
has at least one SFR tracing to it. This is illustrated for

- SFRs that have been newly added or refined within this ST or [20] by checking the rows
   of Table 11, and for SFRs that are merely iterated or simply included due to claims of
   other protection profiles by looking up the rationale of that PP
- for newly introduced security objectives in this ST or [20] by checking the non-cursive
   columns of Table 11 , and for the other security objectives by looking up the rationale
   of that PP.

3706 In other words, in Table 11 , we list only:

- SFRs that have been newly added or refined within this ST or [20]. Mere iterations or
   simple inclusions due to claims of other protection profiles are not listed, however. For
   their coverage we refer to the respective claimed PP.
- Security objectives that are newly introduced in this ST or [20], and their related SFRs.
- Security objectives for the TOE that are affected by the above newly added or refined
   SFRs.

In case an SFR was refined in order to ensure the unified terminology usage, those SFRs arenot listed in Table 11 or justifies below, because these refinements have no security impacts.

Analogously, we limit our justification to the above SFRs and security objectives. For other security objectives, and for the justification of security objectives w.r.t. SFRs that are included or iterated from claimed protection profiles, we refer to the detailed rationales in [5], [6] and [14].

3719 OT.Chip\_Auth\_Proof\_PACE\_CAM is a newly introduced security objective that aims to 3720 ensure the authenticity of the electronic document's chip by the PACE-CAM protocol, in 3721 particular in the context of an ePassport application. This is supported by FCS CKM.1/CAM 3722 for cryptographic key-generation, and FIA API.1/PACE CAM and FCS COP.1/CAM for the 3723 implementation itself, as well as FIA\_UID.1/PACE\_EAC1PP and 3724 FIA\_UAU.5/PACE\_EAC1PP, the latter supporting the PACE protocol.

OT.Chip\_Auth\_Proof\_AA is a newly introduced security objective that aims to ensure the
authenticity of the electronic document's chip by the Active Authentication protocol, in
particular in the context of an ePassport Application. This is supported by FCS\_CKM.1/AA for



3728 cryptographic key generation, and FIA\_API.1/AA, FIA\_UAU.4/PACE\_EAC1PP and
3729 FCS\_COP.1/AA for the implementation itself. The FMT\_MTD.1/KEY\_READ\_EAC1PP
3730 ensures the authenticity of the TOE, because it restricts the ability to read the Active
3731 Authentication private key to none. These do not affect the discussion of the rationale of [5].

The OT.AC\_Pers enforce that all TSF data can be written by authorized Personalisation Agent only and this is supported by **FMT\_MTD.1/AA\_Private\_Key** for the Active Authentication key pair.

FIA\_UAU.1/SSCDPP is refined here in a way that the TOE supports additionally EAC2 based
 access control w.r.t. SSCD-related user data. This does not affect the discussion of the
 rationale of [14].

FDP\_ACF.1/TRM unifies the access control SFPs of FDP\_ACF.1/TRM\_EAC2PP and
FDP\_ACF.1/TRM\_EAC1PP. Both access control SFPs however are maintained w.r.t.
sensitive EAC1-protected data and EAC2-protected data. Thus the discussion of the rationale
of [5] and [6] remains unaffected.

- FMT\_SMR.1/EAC1PP and FMT\_SMR.1/EAC2PP have been unified to FMT\_SMR.1 by
  adding additional roles. For all security objectives affected, FMT\_SMR.1 supports related roles
  analogously as in the discussion of the rationales of [5] and [6].
- The security objective OT.Cap\_Avail\_Loader is directly covered by the SFRs FMT\_LIM.1/Loader and FMT\_LIM.2/Loader, which limits the availability of the loader, as required by the objective.
- 3748 **FPT\_EMS.1/EAC1PP** and **FPT\_EMS.1/EAC2PP** together define all protected data. Since all 3749 previous data are included, the discussion of the rationales of [5] and [6] is not affected.

The objective **OT.Non\_Interfere** aims to ensure that no security related interferences between the implementations of the different access control mechanisms exist that allow unauthorized access of user or TSF-Data. This objective is fulfilled by enforcing the access control SFPs, in particular **FDP\_ACF.1/TRM** in connection with **FDP\_ACC.1/TRM\_EAC1PP**. Related roles are supported by **FMT\_SMR.1**. Interferences that are observable by emissions from the TOE are prevented due to **FPT\_EMS.1/EAC1PP**, **FPT\_EMS.1/EAC2PP**, **and FPT\_EMS.1/SSCDPP**, where the set union of all defined data covers all relevant data.



The security objective **OT.CA2** aims at enabling verification of the authenticity of the TOE as a whole device. This objective is mainly achieved as described in [20]. The secure generation of cryptography key pair is ensured by **FCS\_CKM.1/CA2**.

The security objective **OT.RI\_EAC2** aims at providing a way to pseudonymously identify an electronic document holder without granting a terminal read access to sensitive user data. This objective is mainly achieved as described in [20]. The secure generation of cryptography key pair is ensured by **FCS\_CKM.1/RI**.

## **3764 6.3.2. Rationale for SFR's Dependencies**

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and nondissolved dependencies are appropriately explained.

The dependency analysis has directly been made within the description of each SFR in Section 6.1 above. All dependencies being expected by [2] and by extended components definition in Chapter 5 are either fulfilled, or their non-fulfillment is justified.

## **3772 6.3.3. Security Assurance Requirements Rationale**

3773 The current assurance package was chosen based on the predefined assurance package 3774 EAL4. This package permits a developer to gain maximum assurance from positive security 3775 engineering based on good commercial development practices which, through rigorous, do not 3776 require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level, 3777 at which it is likely to retrofit to an existing product line in an economically feasible way. EAL4 3778 is applicable in those circumstances where developers or users require a moderate to high 3779 level of independently assured security in conventional commodity TOEs and are prepared to 3780 incur additional security specific engineering costs.

The selection of the component ALC\_DVS.2 provides a higher assurance of the security of the electronic document's development and manufacturing, especially for the secure handling of sensitive material.

The selection of the component ATE\_DPT.2 provides a higher assurance than the predefined EAL4 package due to requiring the functional testing of SFR-enforcing modules.



The selection of the component AVA\_VAN.5 provides a higher assurance than the predefined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 3, entry 'Attacker'). This decision represents a part of the conscious security policy for the electronic document required by the electronic document issuer and reflected by the current ST.

The set of assurance requirements being part of EAL4 fulfills all dependencies a priori. The augmentation of EAL4 chosen comprises the following assurance components: ALC\_DVS.2, ATE\_DPT.2 and AVA\_VAN.5. For these additional assurance components, all dependencies are met or exceeded in the EAL4 assurance package. Below we list only those assurance requirements that are additional to EAL4.

- 3797 ALC\_DVS.2
- 3798 Dependencies:
- 3799 None
- 3800 ATE\_DPT.2
- 3801 Dependencies:
- 3802 ADV\_ARC.1, ADV\_TDS.3, ATE\_FUN.1
- 3803 fulfilled by ADV\_ARC.1, ADV\_TDS.3, ATE\_FUN.1
- 3804 AVA\_VAN.5
- 3805 Dependencies:
- 3806 ADV\_ARC.1, ADV\_FSP.4, ADV\_TDS.3, ADV\_IMP.1, AGD\_OPE.1, AGD\_PRE.1,
   3807 ATE\_DPT.1
- fulfilled by ADV\_ARC.1, ADV\_FSP.4, ADV\_TDS.3, ADV\_IMP.1, AGD\_OPE.1,
  AGD\_PRE.1, ATE\_DPT.2
- 3810 6.3.4. Security Requirements Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the



security assurance requirements (SARs) are internally consistent. The analysis of the TOE's
security requirements with regard to their mutual support and internal consistency
demonstrates:

The dependency analysis in Section 6.3.2 for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed and non-satisfied dependencies are appropriately justified.

All subjects and objects addressed by more than one SFR are also treated in a consistent way:
the SFRs impacting them do not require any contradictory property or behavior of these
'shared' items.

3823 The assurance package EAL4 is a predefined set of internally consistent assurance 3824 requirements. The dependency analysis for the sensitive assurance components in Section 3825 6.3.3 shows that the assurance requirements are internally consistent as all (additional) 3826 dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements can only arise due to
functional-assurance dependencies not being met. As shown in Section 6.3.2 and Section
6.3.3, the chosen assurance components are adequate for the functionality of the TOE. Hence,
there are no inconsistencies between the goals of these two groups of security requirements.



- 3831 7. TOE SUMMARY SPECIFICATION
- 3832 **7.1.TOE Security Functions**

#### 3833 7.1.1. TSF.AccessControl

3834 The TOE enforces access control in order to access User Data and TSF-data and maintains 3835 different security roles.

SFR	Description
FIA_AFL.1/Suspend_PIN_EAC2PP	The TSF responsible to suspend the reference value of PIN.
FIA_AFL.1/Block_PIN_EAC2PP	The TSF responsible to block the reference value of PIN.
FIA_AFL.1/SSCDPP	The TSF responsible to block the reference value of RAD.
FIA_UID.1/PACE_EAC2PP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user identification.
FIA_UID.1/EAC2_Terminal_EAC2PP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user identification.
FIA_UAU.1/PACE_EAC2PP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user authentication.
FIA_UAU.1/EAC2_Terminal_EAC2PP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user authentication.
FIA_AFL.1/PACE_EAC2PP	The TSF responsible to delay each following authentication attempt.
FIA_UID.1/PACE_EAC1PP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user identification.
FIA_UAU.1/PACE_EAC1PP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user authentication.
FIA_AFL.1/PACE_EAC1PP	Equivalent to FIA_AFL.1/PACE_EAC2PP.
FIA_UID.1/SSCDPP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user identification.
FIA_UAU.1/SSCDPP	The TSF responsible to restrict other TSF-mediated actions on behalf of that user before the user authentication.
FDP_ACC.1/TRM_EAC2PP	This TSF responsible to enforce the Access Control SFP.
FDP_ACF.1/TRM	This TSF responsible to enforce the Access Control SFP.
FDP_ACC.1/TRM_EAC1PP	Equivalent to FDP_ACC.1/TRM_EAC2PP.
FDP_ACC.1/SCD/SVD_Generation_SSCDPP	This TSF responsible to enforce the SCD/SVD Generation SFP.
FDP_ACF.1/SCD/SVD_Generation_SSCDPP	This TSF responsible to enforce the SCD/SVD Generation SFP.
FDP_ACC.1/SVD_Transfer_SSCDPP	This TSF responsible to enforce the SVD Transfer SFP.
FDP_ACF.1/SVD_Transfer_SSCDPP	This TSF responsible to enforce the SVD Transfer SFP.
FDP_ACC.1/Signature-creation_SSCDPP	This TSF responsible to enforce the Signature Creation SFP.

FDP_ACF.1/Signature-creation_SSCDPP	This TSF responsible to enforce the Signature Creation SFP.
FMT_MTD.1/CVCA_INI_EAC2PP	This TSF responsible to restrict the ability to write certain objects.
FMT_MTD.1/CVCA_UPD_EAC2PP	This TSF responsible to restrict the ability to update certain objects.
FMT_MTD.1/DATE_EAC2PP	This TSF responsible to restrict the ability to modify the current date.
FMT_MTD.1/PA_EAC2PP	This TSF responsible to restrict the ability to write certain objects.
FMT_MTD.1/SK_PICC_EAC2PP	This TSF responsible to restrict the ability to create or load the Chip Authentication private key(s) (SKPICC) and the Restricted Identification Private Key(s).
FMT_MTD.1/KEY_READ_EAC2PP	This TSF responsible to restrict the ability to read certain objects.
FMT_SMR.1	This TSF responsible to maintain the Manufacturer, Personalization Agent, Country Verifying Certification Authority (CVCA), Document Verifier (DV), Terminal, PACE Terminal, EAC2 terminal, if the eID, ePassport and/or eSign application are active, EAC1 terminal, if the ePassport application is active, Electronic Document Holder roles.
FMT_SMR.1/SSCDPP	This TSF responsible to maintain the R.Admin and R.Sigy roles.
FMT_MOF.1/SSCDPP	This TSF responsible to restrict the ability to enable the functions signature creation function.
FMT_MSA.1/Admin_SSCDPP	This TSF responsible to enforce the SCD/SVD Generation SFP.
FMT_MSA.1/SignatorySSCDPP	This TSF responsible to enforce the SCD/SVD Generation SFP.
FMT_MSA.3/SSCDPP	This TSF responsible to enforce the SCD/SVD Generation SFP, SVD Transfer SFP and Signature Creation SFP.
FMT_MTD.1/Admin_SSCDPP	This TSF responsible to restrict the ability to create the RAD.
FMT_MTD.1/Signatory_SSCDPP	This TSF responsible to restrict the ability to modify the RAD
FMT_MTD.1/CVCA_INI_EAC1PP	This TSF responsible to shall restrict the ability to write certain objects.
FMT_MTD.1/CVCA_UPD_EAC1PP	This TSF responsible to restrict the ability to update certain objects.
FMT_MTD.1/DATE_EAC1PP	This TSF responsible to restrict the ability to modify the current date.
FMT_MTD.1/CAPK_EAC1PP	This TSF responsible to restrict the ability to create, load the Chip Authentication Private Key.
FMT_MTD.1/PA_EAC1PP	This TSF responsible to restrict the ability to write the Document Security Object (SOD).
FMT_MTD.1/KEY_READ_EAC1PP	This TSF responsible to restrict the ability to read certain objects.
FMT_MTD.1/AA_Private_Key	This TSF responsible to restrict the ability to create or load the Active Authentication Private Key.

## **3836 7.1.2. TSF.Authenticate**

The TOE supports several authentication mechanism in order to authenticate the Users,Terminals and to prove the genuineness of the electronic document.

The supported mechanism and protocols are based on ICAO and BSI standards [7], [8], [16], and [17] and [18].



3841 Supported authentication mechanism:

3842	٠	Password Authenticated Connection Establishment (PACE) [7], [16], [17].
3843		<ul> <li>Generic Mapping</li> </ul>

- Generic Mapping
  - Chip Authentication Mapping 0
- Active Authentication [7] 3845 •

3844

3851

3852

3853

- Chip Authentication version 1 [16] 3846 •
- Terminal Authentication version 1 [16] 3847 •
- Chip Authentication version 2 [17] 3848 •
- Terminal Authentication version 2 [17] 3849 •
- **Restricted Identification [17]** 3850 ٠
  - Symmetric Authentication (Device authentication) [30] •
    - Symmetric Role Authentication [30] •
    - User Verification [30] •

SFR	Description
FIA_AFL.1/Suspend_PIN_EAC2PP	This TSF responsible for PACE.
FIA_AFL.1/Block_PIN_EAC2PP	This TSF responsible for PACE.
FIA_API.1/CA_EAC2PP	This TSF responsible for Chip Authentication v2.
FIA_API.1/RI_EAC2PP	This TSF responsible for Restricted Identification.
FIA_UID.1/PACE_EAC2PP	This TSF responsible for PACE.
FIA_UID.1/EAC2_Terminal_EAC2PP	This TSF responsible for PACE.
FIA_UAU.1/PACE_EAC2PP	This TSF responsible for PACE.
FIA_UAU.1/EAC2_Terminal_EAC2PP	This TSF responsible for PACE and Terminal Authentication v2.
FIA_UAU.4/PACE_EAC2PP	This TSF responsible for PACE, Terminal Authentication v2 and Symmetric Authentication.
FIA_UAU.5/PACE_EAC2PP	This TSF responsible for PACE, Terminal Authentication v2, Chip Authentication v2 and Symmetric Authentication.
FIA_UAU.6/CA_EAC2PP	This TSF responsible for Chip Authentication v2.
FIA_AFL.1/PACE_EAC2PP	This TSF responsible for PACE.
FIA_UAU.6/PACE_EAC2PP	This TSF responsible for PACE.
FIA_UID.1/PACE_EAC1PP	This TSF responsible for PACE, Chip Authentication v1 and Chip Authentication Mapping (PACE-CAM).
FIA_UAU.1/PACE_EAC1PP	This TSF responsible for PACE, Chip Authentication v1, Terminal Authentication v1 and Chip Authentication Mapping (PACE-CAM).
FIA_UAU.4/PACE_EAC1PP	This TSF responsible for PACE, Symmetric Authentication, Terminal Authentication v1 and Active Authentication.
FIA_UAU.5/PACE_EAC1PP	This TSF responsible for PACE, Chip Authentication Mapping (PACE-CAM), Symmetric Authentication, Terminal Authentication v1.
FIA_UAU.6/EAC_EAC1PP	This TSF responsible for Chip Authentication v1
FIA_API.1/EAC1PP	This TSF responsible for Chip Authentication v1
FIA_API.1/PACE_CAM	This TSF responsible for Chip Authentication Mapping
FIA_API.1/AA	This TSF responsible for Active Authentication
FIA_AFL.1/PACE_EAC1PP	Equivalent to FIA_AFL.1/PACE_EAC2PP.
FIA_UAU.6/PACE_EAC1PP	This TSF responsible for PACE.
FIA_AFL.1/SSCDPP	This TSF responsible for User Verification.
FDP_ACF.1/TRM	This TSF responsible for Terminal Authentication and PACE.
FDP_ACF.1/SCD/SVD_Generation_SSCDPP	This TSF responsible for User Verification



FDP_ACF.1/SVD_Transfer_SSCDPP	This TSF responsible for R.Admin.
FDP_ACF.1/Signature-creation_SSCDPP	This TSF responsible for User Verification.
FTP_ITC.1/PACE_EAC2PP	This TSF responsible for PACE
FTP_ITC.1/CA_EAC2PP	This TSF responsible for Chip Authentication v2
FTP_ITC.1/PACE_EAC1PP	This TSF responsible for PACE.
FMT_MTD.1/CVCA_INI_EAC2PP	This TSF responsible for authentication of the
FINT_NITD.I/CVCA_INI_EAC2PP	Personalisation Agent.
FMT_MTD.1/CVCA_UPD_EAC2PP	This TSF responsible for the authentication of Country Verifying Certification Authority.
FMT_MTD.1/DATE_EAC2PP	This TSF responsible for the authentication of CVCA, DV and the EAC2 Terminal
FMT_MTD.1/PA_EAC2PP	This TSF responsible for authentication of Personalization Agent.
FMT_MTD.1/SK_PICC_EAC2PP	This TSF responsible for authentication of the Personalisation Agent.
FMT_MTD.1/Initialize_PIN_EAC2PP	This TSF responsible for authentication of the Personalisation Agent.
FMT_MTD.1/Change_PIN_EAC2PP	This TSF responsible for authentication of Document Holder and the EAC2 Terminal (with Terminal Authorisation level for PIN management).
FMT_MTD.1/Resume_PIN_EAC2PP	This TSF responsible for authentication of Document Holder
FMT_MTD.1/Unblock_PIN_EAC2PP	This TSF responsible for authentication of Document Holder and the EAC2 Terminal (with Terminal Authorisation level for PIN management).
FMT_MTD.1/Activate_PIN_EAC2PP	This TSF responsible for authentication of the EAC2 Terminal (with Terminal Authorisation level for PIN management).
FMT_MTD.3/EAC2PP	This TSF responsible for the Terminal Authentication v2.
FMT_SMF.1/SSCDPP	This TSF responsible to provide the security functions.
FMT_MOF.1/SSCDPP	This TSF responsible for authentication of R.Sigy
FMT_MSA.1/Admin_SSCDPP	This TSF responsible for authentication of R.Admin
FMT_MSA.1/SignatorySSCDPP	This TSF responsible for authentication of R.Sigy
FMT_MSA.3/SSCDPP	This TSF responsible for authentication of R.Sigy and R.Admin
FMT_MSA.4/SSCDPP	This TSF responsible for authentication of R.Sigy and R.Admin
FMT_MTD.1/Admin_SSCDPP	This TSF responsible for authentication of R.Admin
FMT_MTD.1/Signatory_SSCDPP	This TSF responsible for authentication of R.Sigy
FMT_MTD.1/CVCA_INI_EAC1PP	This TSF responsible for authentication of Personalization Agent.
FMT_MTD.1/CVCA_UPD_EAC1PP	This TSF responsible for authentication of Country Verifying Certification Authority.
FMT_MTD.1/DATE_EAC1PP	This TSF responsible to equivalent to FMT_MTD.1/DATE_EAC2PP.
FMT_MTD.1/CAPK_EAC1PP	This TSF responsible for This TSF responsible for authentication of Personalization Agent or the Manufacturer.
FMT_MTD.1/PA_EAC1PP	This TSF responsible for authentication of Personalization Agent.
FMT_MTD.1/AA_Private_Key	This TSF responsible for authentication of Personalization Agent.
FMT_MTD.3/EAC1PP	This TSF responsible for the Terminal Authentication v2.



#### 3854

## 7.1.3. TSF.SecureManagement

The TOE enforces the secure management of the security attributes, data and functions. 3855 Furthermore the TOE restricts the available commands in each TOE life-cycle phase. 3856

SFR	Description
FMT_MTD.1/CVCA_INI_EAC2PP	This TSF responsible to evaluate whether the Personalisation Agent is authenticated, and it has right to write initial CVCA Public Key, meta-data of the initial CVCA Certificate and initial Current Date.
FMT_MTD.1/CVCA_UPD_EAC2PP	This TSF responsible to evaluate whether the Country Verifying Certification Authority is authenticated, and it has right to update CVCA Public Key (PKCVCA) and meta-data of the CVCA Certificate.
FMT_SMF.1/EAC2PP	This TSF responsible to provide part of the security functions.
FMT_MTD.1/DATE_EAC2PP	This TSF responsible to evaluate whether a CVCA, Document Verifier, or an EAC2 terminal is authenticated and it has right to modify Current Date.
FMT_MTD.1/PA_EAC2PP	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to write the card/chip security object(s) (SO <sub>c</sub> ) and the document Security Object (SO <sub>D</sub> ).
FMT_MTD.1/SK_PICC_EAC2PP	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to create or load the Chip Authentication private key(s) (SKPICC) and the Restricted Identification Private Key(s).
FMT_MTD.1/KEY_READ_EAC2PP	This TSF responsible to restrict the ability to read certain objects.
FMT_MTD.1/Initialize_PIN_EAC2PP	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to write the initial PIN and PUK
FMT_MTD.1/Change_PIN_EAC2PP	This TSF responsible to evaluate whether an Electronic Document Holder is authenticated with PUK or a Terminal with Terminal Authorisation level for PIN management is authenticated and it has right to change the blocked PIN.
FMT_MTD.1/Resume_PIN_EAC2PP	This TSF responsible to evaluate whether an Electronic Document Holder is authenticated, and it has right to resume the suspended PIN.
FMT_MTD.1/Unblock_PIN_EAC2PP	This TSF responsible to evaluate whether an Electronic Document Holder is authenticated with PUK or a Terminal with Terminal Authorisation level for PIN management is authenticated and it has right to unblock the blocked PIN.
FMT_MTD.1/Activate_PIN_EAC2PP	This TSF responsible to evaluate whether a Terminal with Terminal Authorisation level for PIN management is authenticated and it has right to activate or deactivate the PIN.
FMT_SMF.1/SSCDPP	This TSF responsible to provide part of the security functions.
FMT_MOF.1/SSCDPP	This TSF responsible to evaluate whether a R.Sigy is authenticated and it has right to enable the signature creation function.
FMT_MSA.1/Admin_SSCDPP	This TSF responsible to evaluate whether a R.Admin is authenticated and it has right to modify the SCD/SVD management security attribute.

FMT_MSA.1/SignatorySSCDPP	This TSF responsible to evaluate whether a R.Sigy is authenticated and it has right to modify the SCD/SVD operational security attribute.
FMT_MSA.2/SSCDPP	This TSF responsible to ensure that only secure values are accepted for SCD/SVD Management and SCD operational
FMT_MSA.3/SSCDPP	This TSF responsible to provide restrictive default values for security attributes.
FMT_MSA.4/SSCDPP	This TSF responsible for security attribute value inheritance.
FMT_MTD.1/Admin_SSCDPP	This TSF responsible to evaluate whether a R.Admin is authenticated, and it has right to create the RAD.
FMT_MTD.1/Signatory_SSCDPP	This TSF responsible to evaluate whether a R.Sigy is authenticated and it has right to modify the RAD.
FMT_MTD.1/CVCA_INI_EAC1PP	This TSF responsible to evaluate whether the Personalisation Agent is authenticated, and it has right to write initial Country Verifying Certification Authority Public Key, initial Country Verifying Certification Authority Certificate, initial Current Date.
FMT_MTD.1/CVCA_UPD_EAC1PP	This TSF responsible to evaluate whether the Country Verifying Certification Authority is authenticated, and it has right to update Country Verifying Certification Authority Public Key, Country Verifying Certification Authority Certificate.
FMT_SMF.1/EAC1PP	This TSF responsible to provide part of the security functions.
FMT_MTD.1/DATE_EAC1PP	This TSF responsible to equivalent to FMT_MTD.1/DATE_EAC2PP.
FMT_MTD.1/CAPK_EAC1PP	This TSF responsible to evaluate whether a Personalisation Agent or Manufacturer is authenticated, and it has right to create or load the Chip Authentication private key.
FMT_MTD.1/PA_EAC1PP	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to write the document Security Object (SOD).
FMT_MTD.1/KEY_READ_EAC1PP	This TSF responsible to restrict the ability to read cryptographic keys.
FMT_MTD.1/AA_Private_Key	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to create or load the Active Authentication Private Key.

## 3857 **7.1.4. TSF.CryptoKey**

3858 The TOE uses several cryptographic services such as digital signature creation and 3859 verification, asymmetric and symmetric cryptography, random number generation and 3860 complete key management.

3861 Furthermore TSF.CryptoKey provides the secure messaging for the TOE.

SFR	Description
FCS_CKM.1/DH_PACE_EAC2PP	This TSF responsible the Applet part of key agreement for PACE.
FCS_COP.1/SHA_EAC2PP	This TSF responsible the Applet part of hash generation.
FCS_COP.1/SIG_VER_EAC2PP	This TSF responsible the Applet part of digital signature verification.
FCS_COP.1/PACE_ENC_EAC2PP	This TSF responsible the Applet part of secure messaging – encryption and decryption.
FCS_COP.1/PACE_MAC_EAC2PP	This TSF responsible the Applet part of secure messaging – message authentication code.

FCS_CKM.4/EAC2PP	This TSF responsible the Applet part of cryptographic
FCS_RND.1/EAC2PP	key destruction. This TSF responsible the Applet part of random
FCS_CKM.1/DH_PACE_EAC1PP	number generation. This TSF responsible the Applet part of key agreement for PACE.
FCS_CKM.4/EAC1PP	Equivalent to FCS_CKM.4/EAC2PP.
FCS_COP.1/PACE_ENC_EAC1PP	This TSF responsible the Applet part of secure
res_cor.i/racl_lnc_lacirr	messaging – encryption and decryption.
FCS_COP.1/PACE_MAC_EAC1PP	This TSF responsible the Applet part of secure
	messaging – message authentication code.
FCS_RND.1/EAC1PP	Equivalent to FCS_RND.1/EAC2PP.
FCS_CKM.1/CA_EAC1PP	This TSF responsible the Applet part of key agreement for Chip Authentication v1.
FCS_COP.1/CA_ENC_EAC1PP	This TSF responsible the Applet part of secure messaging – encryption and decryption.
FCS_COP.1/SIG_VER_EAC1PP	This TSF responsible the Applet part of digital signature verification.
FCS_COP.1/CA_MAC_EAC1PP	This TSF responsible the Applet part of secure
	messaging – message authentication code.
FCS_CKM.1/CA2	This TSF responsible the Applet part of Chip Authentication version 2 Key pair(s) generation.
FCS_CKM.1/RI	This TSF responsible the Applet part of Restricted
	Identification Key pair (s) generation.
FCS_CKM.1/AA	This TSF responsible the Applet part of Active
	Authentication Key Pair generation.
FCS_COP.1/AA	This TSF responsible the Applet part of digital signature generation.
FCS_CKM.1/CAM	This TSF responsible the Applet part of PACE-CAM
	protocol implementation.
FCS_COP.1/CAM	This TSF responsible the Applet part of PACE-CAM protocol implementation.
FCS_CKM.1/SSCDPP	This TSF responsible the Applet part of SCD/SVD pair generation.
FCS_COP.1/SSCDPP	This TSF responsible the Applet part of digital
	signature creation.
FIA_API.1/CA_EAC2PP	This TSF responsible the Applet part of cryptographic operation for Chip Authentication v2.
FIA_API.1/RI_EAC2PP	This TSF responsible the Applet part of cryptographic
	operation for Restricted Identification.
FIA_API.1/EAC1PP	This TSF responsible the Applet part of cryptographic
	operation for Chip Authentication v1.
FIA_API.1/PACE_CAM	This TSF responsible the Applet part of cryptographic operation for Chip Authentication Mapping.
FIA_API.1/AA	This TSF responsible the Applet part of cryptographic
····· <b>_·</b> ··· <b>_·</b> ··· <b>_·</b> ···	operation for Active Authentication.
FDP_RIP.1/EAC2PP	This TSF responsible to call the Platform functionalities to destroy cryptographic keys.
FDP_UCT.1/TRM_EAC2PP	This TSF responsible the Applet part of secure
	messaging. This TSF responsible the Applet part of secure
FDP_UIT.1/TRM_EAC2PP	messaging.
FDP_RIP.1/EAC1PP	This TSF responsible to call the Platform functionalities
FDP_UCT.1/TRM_EAC1PP	to destroy cryptographic keys. Equivalent to FDP_UCT.1/TRM_EAC2PP.
	Equivalent to FDP_UIT.1/TRM_EAC2PP.
FDP_UIT.1/TRM_EAC1PP	This TSF responsible the Applet part of de-allocation
FDP_RIP.1/SSCDPP	of the resource SCD.
FTP_ITC.1/PACE_EAC2PP	This TSF responsible the Applet part of cryptographic
	operation for trusted channel.



FTP_ITC.1/CA_EAC2PP	This TSF responsible the Applet part of cryptographic operation for trusted channel.
FTP_ITC.1/PACE_EAC1PP	This TSF responsible the Applet part of cryptographic operation for trusted channel.

## 3862 7.1.5. TSF.AppletParametersSign

3863 The TOE enforces the integrity of itself in each life cycle phases.

SFR	Description
FPT_TST.1/EAC2PP	This TSF responsible for initial start-up, periodically during normal operation testing.
FPT_TST.1/EAC1PP	Equivalent to FPT_TST.1/EAC2PP.
FPT_TST.1/SSCDPP	Subsumed by FPT_TST.1/EAC2PP.

#### **3864 7.1.6. TSF.Platform**

The TOE relies on the certified functions and services of the Platform. This TSF is collection of those SFRs, which are uses these functions and services.

SFR	Description
FCS_CKM.1/DH_PACE_EAC2PP	This TSF responsible the Platform part of key
	agreement for PACE.
FCS_COP.1/SHA_EAC2PP	This TSF responsible the Platform part of hash
	generation. This TSF responsible the Platform part of digital
FCS_COP.1/SIG_VER_EAC2PP	signature verification.
FCS_COP.1/PACE_ENC_EAC2PP	This TSF responsible the Platform part of secure
	messaging – encryption and decryption.
FCS_COP.1/PACE_MAC_EAC2PP	This TSF responsible the Platform part of secure
, , , , , , , , , , , , , , , , , , , ,	messaging – message authentication code.
FCS_CKM.4/EAC2PP	This TSF responsible the Platform part of
	cryptographic key destruction.
FCS_RND.1/EAC2PP	This TSF responsible the Platform part of random
	number generation. This TSF responsible the Platform part of key
FCS_CKM.1/DH_PACE_EAC1PP	agreement for PACE.
FCS_CKM.4/EAC1PP	Equivalent to FCS_CKM.4/EAC2PP.
	This TSF responsible the Platform part of secure
FCS_COP.1/PACE_ENC_EAC1PP	messaging – encryption and decryption.
FCS_COP.1/PACE_MAC_EAC1PP	This TSF responsible the Platform part of secure
	messaging – message authentication code.
FCS_RND.1/EAC1PP	Equivalent to FCS_RND.1/EAC2PP.
FCS_CKM.1/CA_EAC1PP	This TSF responsible the Platform part of key
	agreement for Chip Authentication v1.
FCS_COP.1/CA_ENC_EAC1PP	This TSF responsible the Platform part of secure
	messaging – encryption and decryption.
FCS_COP.1/SIG_VER_EAC1PP	This TSF responsible the Platform part of digital
	signature verification. This TSF responsible the Platform part of secure
FCS_COP.1/CA_MAC_EAC1PP	messaging – message authentication code.
FCS_CKM.1/CA2	This TSF responsible the Platform part of Chip
	Authentication version 2 Key pair(s) generation.
FCS_CKM.1/RI	This TSF responsible the Platform part of Restricted
	Identification Key pair(s) generation.
FCS_CKM.1/AA	This TSF responsible the Platform part of Active
	Authentication Key Pair generation.

	This TSF responsible the Platform part of digital
FCS_COP.1/AA	signature generation.
FCS_CKM.1/CAM	This TSF responsible the Platform part of PACE-CAM protocol implementation.
FCS_COP.1/CAM	This TSF responsible the Platform part of PACE-CAM protocol implementation.
FCS_CKM.1/SSCDPP	This TSF responsible the Platform part of SCD/SVD pair generation.
FCS_CKM.4/SSCDPP	This TSF responsible the Platform part of cryptographic key destruction.
FCS_COP.1/SSCDPP	This TSF responsible the Platform part of digital signature creation.
FIA_API.1/CA_EAC2PP	This TSF responsible the Platform part of cryptographic operation for Chip Authentication v2.
FIA_API.1/RI_EAC2PP	This TSF responsible the Platform part of cryptographic operation for Restricted Identification.
FIA_UID.1/PACE_EAC2PP	This TSF responsible for the identifier data of the TOE.
FIA_UID.1/EAC2_Terminal_EAC2PP	This TSF responsible for the identifier data of the TOE.
FIA_UAU.1/PACE_EAC2PP	This TSF responsible for the identifier data of the TOE.
FIA_UAU.1/EAC2_Terminal_EAC2PP	This TSF responsible for the identifier data of the TOE.
FIA_UID.1/PACE_EAC1PP	This TSF responsible for the identifier data of the TOE.
FIA_UAU.1/PACE_EAC1PP	This TSF responsible for the identifier data of the TOE.
FIA_UAU.4/PACE_EAC2PP	This TSF responsible for fresh random numbers for PACE, Terminal Authentication v2 and Symmetric Authentication.
FIA_UAU.5/PACE_EAC2PP	This TSF responsible for Platform part of cryptographic operation for PACE, Terminal Authentication v2, Chip Authentication v2 and Symmetric Authentication.
FIA_UAU.6/CA_EAC2PP	This TSF responsible for Platform part of cryptographic operation for Chip Authentication v2.
FIA_UAU.6/PACE_EAC2PP	This TSF responsible for Platform part of cryptographic operation for PACE.
FIA_UAU.4/PACE_EAC1PP	This TSF responsible for Platform part of cryptographic operation for PACE, Symmetric Authentication, Terminal Authentication v1 and Active Authentication.
FIA_UAU.5/PACE_EAC1PP	This TSF responsible for Platform part of cryptographic operation for PACE, Chip Authentication Mapping (PACE-CAM), Symmetric Authentication, Terminal Authentication v1.
FIA_UAU.6/PACE_EAC1PP	This TSF responsible for Platform part of cryptographic operation for PACE.
FIA_UAU.6/EAC_EAC1PP	This TSF responsible for Platform part of cryptographic operation for Chip Authentication v1
FIA_API.1/EAC1PP	This TSF responsible the Platform part of cryptographic operation for Chip Authentication v1.
FIA_API.1/PACE_CAM	This TSF responsible the Platform part of cryptographic operation for Chip Authentication Mapping.
FIA_API.1/AA	This TSF responsible the Platform part of cryptographic operation for Active Authentication.
FDP_RIP.1/EAC2PP	This TSF responsible to make unavailable any cryptographic data used in runtime cryptographic computations.
FDP_UCT.1/TRM_EAC2PP	This TSF responsible the Platform part of secure messaging.
FDP_UIT.1/TRM_EAC2PP	This TSF responsible the Platform part of secure messaging.
FDP_RIP.1/EAC1PP	This TSF responsible to make unavailable any cryptographic data used in runtime cryptographic computations.
FDP_UCT.1/TRM_EAC1PP	Equivalent to FDP_UCT.1/TRM_EAC2PP.

of the resource SCD.         FDP_SDI.2/Persistent_SSCDPP         FAU_SAS.1/EAC2PP         This TSF responsible for integrity of user data.         FAU_SAS.1/EAC2PP         This TSF responsible to store the Initialisation and Pre Personalisation Data in the audit records         FAU_SAS.1/EAC2PP         FMT_SMR.1         This TSF responsible to provide part of the securit roles.         FMT_LIM.1/EAC2PP         FMT_LIM.2/EAC2PP         This TSF responsible to limit its capabilities to enforce the policy as described in the SFR.         FMT_LIM.2/EAC2PP         This TSF responsible to restrict the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer.         FMT_MTD.1/INI_ENA_EAC2PP         This TSF responsible to restrict the ability to read on the Initialisation Data and the Pre-personalisation Data to the Manufacturer.         FMT_SMF.1/EAC2PP         This TSF responsible to provide part of the securit functions.         FMT_SMF.1/EAC2PP         This TSF responsible to provide part of the securit functions.         FMT_SMF.1/EAC2PP         This TSF responsible to provide part of the securit functions.         FMT_SMF.1/EAC2PP         This TSF responsible to provide part of the securit functions.         FMT_SMF.1/EAC2PP         FMT_LIM.1/EAC1PP         Equivalent to FMT_LIM.2/EAC2	FDP_RIP.1/SSCDPP FDP_SDI.2/Persistent_SSCDPP FDP_SDI.2/DTBS_SSCDPP	
FDP_SDI.2/Persistent_SSCDPP       This TSF responsible for integrity of user data.         FDP_SDI.2/DTBS_SSCDPP       This TSF responsible to store the Initialisation and Pre- Personalisation Data in the audit records         FAU_SAS.1/EAC1PP       Equivalent to FAU_SAS.1/EAC2PP.         FMT_SMR.1       This TSF responsible to provide part of the securit roles.         FMT_LIM.1/EAC2PP       This TSF responsible to limit its capabilities to enford the policy as described in the SFR.         FMT_LIM.2/EAC2PP       This TSF responsible to restrict the ability to enford the policy as described in the SFR.         FMT_MTD.1/INI_ENA_EAC2PP       This TSF responsible to restrict the ability to enford the policy as described in the SFR.         FMT_MTD.1/INI_ENA_EAC2PP       This TSF responsible to restrict the ability to enford the policy as described in the SFR.         FMT_MTD.1/INI_ENA_EAC2PP       This TSF responsible to restrict the ability to enford the policy as described in the SFR.         FMT_MTD.1/INI_DIS_EAC2PP       This TSF responsible to restrict the ability to read or the Initialisation Data and the Pre-personalisation Data to the Manufacturer.         FMT_SMF.1/EAC2PP       This TSF responsible to provide part of the securit functions.         FMT_LIM.1/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_LIM.2/EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_LIM.1/EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_LIM.1/EAC1PP       Equivalent to FMT_LIM.2/EAC2	FDP_SDI.2/DTBS_SSCDPP	
FDP_SDI.2/DTBS_SSCDPP       This TSF responsible for integrity of user data.         FAU_SAS.1/EAC2PP       This TSF responsible to store the Initialisation and Pre-Personalisation Data in the audit records         FAU_SAS.1/EAC1PP       Equivalent to FAU_SAS.1/EAC2PP.         FMT_SMR.1       This TSF responsible to provide part of the securit roles.         FMT_LIM.1/EAC2PP       This TSF responsible to limit its capabilities to enford the policy as described in the SFR.         FMT_LIM.2/EAC2PP       This TSF responsible to is securit its availability to enford the policy as described in the SFR.         FMT_MTD.1/INI_ENA_EAC2PP       This TSF responsible to restrict the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer.         FMT_MTD.1/INI_DIS_EAC2PP       This TSF responsible to provide part of the securit functions.         FMT_SMF.1/EAC2PP       This TSF responsible to provide part of the securit functions.         FMT_SMF.1/EAC2PP       This TSF responsible to provide part of the securit functions.         FMT_SMF.1/EAC2PP       This TSF responsible to provide part of the securit functions.         FMT_SMF.1/EAC2PP       This TSF responsible to provide part of the securit functions.         FMT_SMF.1/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_LIM.1/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_LIM.2/EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_LIM.1/EAC1PP       Equivalent	FDP_SDI.2/DTBS_SSCDPP	This TSF Tesponsible for integrity of user data.
FAU_SAS.1/EAC2PP       This TSF responsible to store the Initialisation and Pre         FAU_SAS.1/EAC1PP       Equivalent to FAU_SAS.1/EAC2PP.         FMT_SMR.1       This TSF responsible to provide part of the securit roles.         FMT_LIM.1/EAC2PP       This TSF responsible to limit its capabilities to enforce the policy as described in the SFR.         FMT_LIM.2/EAC2PP       This TSF responsible to limit its availability to enforce the policy as described in the SFR.         FMT_LIM.2/EAC2PP       This TSF responsible to restrict the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer.         FMT_MTD.1/INI_DIS_EAC2PP       This TSF responsible to restrict the ability to read on the Initialisation Data and Pre-personalisation Data to the Manufacturer.         FMT_SMF.1/EAC2PP       This TSF responsible to provide part of the securit functions.         FMT_SMF.1/EAC2PP       This TSF responsible to previde part of the securit functions.         FMT_SMF.1/EAC2PP       This TSF responsible to provide part of the securit functions.         FMT_SMF.1/EAC2PP       This TSF responsible to provide part of the securit functions.         FMT_LIM.1/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_LIM.2/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_LIM.1/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_LIM.1/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_LIM.1/EAC1PP       Equivalent to FMT_		This TSE responsible for integrity of upor date
Personalisation Data in the audit records         FAU_SAS.1/EAC1PP       Equivalent to FAU_SAS.1/EAC2PP.         FMT_SMR.1       This TSF responsible to provide part of the securit roles.         FMT_LIM.1/EAC2PP       This TSF responsible to limit its capabilities to enforce the policy as described in the SFR.         FMT_LIM.2/EAC2PP       This TSF responsible to limit its availability to enforce the policy as described in the SFR.         FMT_LIM.2/EAC2PP       This TSF responsible to restrict the ability to enforce the policy as described in the SFR.         FMT_MTD.1/INI_ENA_EAC2PP       This TSF responsible to restrict the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer.         FMT_MTD.1/INI_DIS_EAC2PP       This TSF responsible to restrict the ability to read or the Initialisation Data and the Pre-personalisation Data to the Manufacturer.         FMT_SMF.1/EAC2PP       This TSF responsible to provide part of the securit functions.         FMT_SMF.1/EAC1PP       This TSF responsible to provide part of the securit functions.         FMT_LIM.1/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MT_MTD.1/INI_DIS_EAC1PP       Equivalent t		
FMT_SMR.1       This TSF responsible to provide part of the securit roles.         FMT_LIM.1/EAC2PP       This TSF responsible to limit its capabilities to enford the policy as described in the SFR.         FMT_LIM.2/EAC2PP       This TSF responsible to limit its availability to enford the policy as described in the SFR.         FMT_MTD.1/INI_ENA_EAC2PP       This TSF responsible to restrict the ability to enford the policy as described in the SFR.         FMT_MTD.1/INI_DIS_EAC2PP       This TSF responsible to restrict the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer.         FMT_SMF.1/EAC2PP       This TSF responsible to restrict the ability to read on the Initialisation Data and the Pre-personalisation Data to the Personalisation Agent.         FMT_SMF.1/EAC2PP       This TSF responsible to provide part of the securit functions.         FMT_LIM.1/EAC1PP       This TSF responsible to provide part of the securit functions.         FMT_LIM.1/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.		Personalisation Data in the audit records
roles.         FMT_LIM.1/EAC2PP       This TSF responsible to limit its capabilities to enford the policy as described in the SFR.         FMT_LIM.2/EAC2PP       This TSF responsible to limit its availability to enford the policy as described in the SFR.         FMT_MTD.1/INI_ENA_EAC2PP       This TSF responsible to restrict the ability to write the lnitialisation Data and Pre-personalisation Data to the Manufacturer.         FMT_MTD.1/INI_DIS_EAC2PP       This TSF responsible to restrict the ability to read on the Initialisation Data and the Pre-personalisation Data to the Initialisation Data and the Pre-personalisation Data to the Personalisation Agent.         FMT_SMF.1/EAC2PP       This TSF responsible to provide part of the securit functions.         FMT_SMF.1/EAC1PP       This TSF responsible to provide part of the securit functions.         FMT_LIM.2/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       This TSF ensures that d	FAU_SAS.1/EAC1PP	•
the policy as described in the SFR.         FMT_LIM.2/EAC2PP       This TSF responsible to limit its availability to enford the policy as described in the SFR.         FMT_MTD.1/INI_ENA_EAC2PP       This TSF responsible to restrict the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer.         FMT_MTD.1/INI_DIS_EAC2PP       This TSF responsible to restrict the ability to read of the Initialisation Data and the Pre-personalisation Data to the Personalisation Agent.         FMT_SMF.1/EAC2PP       This TSF responsible to provide part of the securit functions.         FMT_SMF.1/EAC1PP       This TSF responsible to provide part of the securit functions.         FMT_LIM.1/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_LIM.2/EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP<	FMT_SMR.1	
FMT_MTD.1/INI_ENA_EAC2PP       This TSF responsible to restrict the ability to write the lnitialisation Data and Pre-personalisation Data to the Manufacturer.         FMT_MTD.1/INI_DIS_EAC2PP       This TSF responsible to restrict the ability to read on the Initialisation Data and the Pre-personalisation Data to the Manufacturer.         FMT_SMF.1/EAC2PP       This TSF responsible to restrict the ability to read on the Initialisation Data and the Pre-personalisation Data to the Personalisation Agent.         FMT_SMF.1/EAC2PP       This TSF responsible to provide part of the securities functions.         FMT_SMF.1/EAC1PP       This TSF responsible to provide part of the securities functions.         FMT_LIM.1/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.         FPT_EMS.1/EAC2PP       This TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) that might disclose cryptographic keys.	FMT_LIM.1/EAC2PP	This TSF responsible to limit its capabilities to enforce the policy as described in the SFR.
Initialisation Data and Pre-personalisation Data to th Manufacturer.FMT_MTD.1/INI_DIS_EAC2PPThis TSF responsible to restrict the ability to read or the Initialisation Data and the Pre-personalisation Data to the Personalisation Agent.FMT_SMF.1/EAC2PPThis TSF responsible to provide part of the securit functions.FMT_SMF.1/EAC1PPThis TSF responsible to provide part of the securit functions.FMT_LIM.1/EAC1PPEquivalent to FMT_LIM.1/EAC2PP.FMT_LIM.2/EAC1PPEquivalent to FMT_LIM.2/EAC2PP.FMT_MTD.1/INI_ENA_EAC1PPEquivalent to FMT_LIM.2/EAC2PP.FMT_MTD.1/INI_ENA_EAC1PPEquivalent to FMT_MTD.1/INI_ENA_EAC2PP.FMT_MTD.1/INI_DIS_EAC1PPEquivalent to FMT_MTD.1/INI_DIS_EAC2PP.FMT_MTD.1/INI_DIS_EAC1PPEquivalent to FMT_MTD.1/INI_DIS_EAC2PP.FPT_EMS.1/EAC2PPThis TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timin (measurable at e. g. electrical contacts) that migli disclose cryptographic keys.	FMT_LIM.2/EAC2PP	This TSF responsible to limit its availability to enforce the policy as described in the SFR.
FMT_SMF.1/EAC2PP       the Initialisation Data and the Pre-personalisation Data to the Personalisation Agent.         FMT_SMF.1/EAC1PP       This TSF responsible to provide part of the securit functions.         FMT_LIM.1/EAC1PP       This TSF responsible to provide part of the securit functions.         FMT_LIM.2/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.         FMT_EMS.1/EAC2PP       This TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timin (measurable at e. g. electrical contacts) that might disclose cryptographic keys.	FMT_MTD.1/INI_ENA_EAC2PP	
functions.         FMT_SMF.1/EAC1PP       This TSF responsible to provide part of the securit functions.         FMT_LIM.1/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_LIM.2/EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.         FPT_EMS.1/EAC2PP       This TSF ensures that during command executio there are no usable variations in power consumptio (measurable at e. g. electrical contacts) or timin (measurable at e. g. electrical contacts) that might disclose cryptographic keys.	FMT_MTD.1/INI_DIS_EAC2PP	
functions.         FMT_LIM.1/EAC1PP       Equivalent to FMT_LIM.1/EAC2PP.         FMT_LIM.2/EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.         FPT_EMS.1/EAC2PP       This TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timin (measurable at e. g. electrical contacts) that might disclose cryptographic keys.	FMT_SMF.1/EAC2PP	functions.
FMT_LIM.2/EAC1PP       Equivalent to FMT_LIM.2/EAC2PP.         FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.         FPT_EMS.1/EAC2PP       This TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timin (measurable at e. g. electrical contacts) that might disclose cryptographic keys.	FMT_SMF.1/EAC1PP	functions.
FMT_MTD.1/INI_ENA_EAC1PP       Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.         FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.         FPT_EMS.1/EAC2PP       This TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timin (measurable at e. g. electrical contacts) that might disclose cryptographic keys.	FMT_LIM.1/EAC1PP	
FMT_MTD.1/INI_DIS_EAC1PP       Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.         FPT_EMS.1/EAC2PP       This TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timin (measurable at e. g. electrical contacts) that might disclose cryptographic keys.	FMT_LIM.2/EAC1PP	-
FPT_EMS.1/EAC2PP       This TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timin (measurable at e. g. electrical contacts) that might disclose cryptographic keys.	FMT_MTD.1/INI_ENA_EAC1PP	Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.
there are no usable variations in power consumptio (measurable at e. g. electrical contacts) or timin (measurable at e. g. electrical contacts) that migl disclose cryptographic keys.	FMT_MTD.1/INI_DIS_EAC1PP	Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.
	FPT_EMS.1/EAC2PP	there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timing (measurable at e. g. electrical contacts) that might
the failures occur.	FPT_FLS.1/EAC2PP	
FPT_TST.1/EAC2PP         This TSF responsible for the integrity of stored TS executable code.	FPT_TST.1/EAC2PP	This TSF responsible for the integrity of stored TSF executable code.
<b>FPT_PHP.3/EAC2PP</b> This TSF ensures resistance to physical attack.	FPT_PHP.3/EAC2PP	This TSF ensures resistance to physical attack.
<b>FPT_TST.1/EAC1PP</b> Equivalent to FPT_TST.1/EAC2PP.	FPT_TST.1/EAC1PP	Equivalent to FPT_TST.1/EAC2PP.
<b>FPT_FLS.1/EAC1PP</b> Equivalent to FPT_FLS.1/EAC2PP.	FPT_FLS.1/EAC1PP	Equivalent to FPT_FLS.1/EAC2PP.
FPT_PHP.3/EAC1PPEquivalent to FPT_PHP.3/EAC2PP	FPT_PHP.3/EAC1PP	Equivalent to FPT_PHP.3/EAC2PP
there are no usable variations in power consumptio (measurable at e. g. electrical contacts) or timin (measurable at e. g. electrical contacts) that migh disclose cryptographic keys.	FPT_EMS.1/EAC1PP	
there are no usable variations in power consumptio (measurable at e. g. electrical contacts) or timin (measurable at e. g. electrical contacts) that migl disclose cryptographic keys.	FPT_EMS.1/SSCDPP	This TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timing (measurable at e. g. electrical contacts) that might disclose cryptographic keys.
<b>FPT_FLS.1/SSCDPP</b> Equivalent to FPT_FLS.1/EAC2PP.	FPT_FLS.1/SSCDPP	
attack.	FPT_PHP.1/SSCDPP	
FPT_PHP.3/SSCDPPSubsumed by FPT_PHP.3/EAC2PP.	FPT_PHP.3/SSCDPP	Subsumed by FPT_PHP.3/EAC2PP.
FPT_TST.1/SSCDPP Subsumed by FPT_TST.1/EAC2PP.		Subsumed by FPT_TST.1/EAC2PP.
	FPT_TST.1/SSCDPP	

#### FMT\_LIM.2/Loader

This TSF responsible to limit its availability to enforce the policy as described in the SFR.

#### **3867 7.2.Assurance Measures**

- 3868 This section describes the Assurance Measures fulfilling the requirements listed in section 6.2.
- 3869 The following table lists the Assurance measures and references the corresponding
- 3870 documents describing the measures.

Description
The representing of the TSF is described in the documentation for functional specification, in the documentation for TOE design, in the security architecture description and in the documentation for implementation representation.
The guidance documentation is described in the User's Guide documentation [22] and the Administrator's Guide documentation [21].
The life-cycle support of the TOE during its development and maintenance is described in the life-cycle documentation including configuration management, delivery procedures, development security as well as development tools.
The testing of the TOE is described in the test documentation.
The vulnerability assessment for the TOE is described in the vulnerability analysis documentation. e measures and corresponding documents

## 3872 **7.3.Fulfillment of the SFRs**

3871

3873 The following table shows the mapping of the SFRs to security functions of the TOE:



TOE SFR / Security Function					u	
			Ħ		rSF.AppletParametersSign	
			me		ers	
	0		<mark>g</mark> en		lete	
	, inter-	ate	na	<u> </u>	am	
	ပို	tic	Ma	(e)	ar	F
	SS	en		<b>to</b>	etF	orr
	ő	nth	Scl	ζ	ldd	atf
	Ă.	. Ai	, Š	SF.CryptoKey	- A	d.
	<b>TSF.AccessControl</b>	<b>TSF.A</b> uthenticate	<b>TSF.SecureManagement</b>	LS L	5 S	<b>ISF.</b> Platform
FCS_CKM.1/DH_PACE_EAC2P P	-	- ·	-	X	-	Х
FCS COP.1/SHA EAC2PP	-	-	_	Х	-	Х
FCS_COP.1/SIG_VER_EAC2PP	-	-	-	X	-	X
FCS_COP.1/PACE_ENC_EAC2P	-	-	-	X	-	X
P						
FCS_COP.1/PACE_MAC_EAC2 PP	-	-	-	Х	-	Х
FCS_CKM.4/EAC2PP	-	-	-	Х	-	Х
FCS_RND.1/EAC2PP	-	-	-	Х	-	Х
FCS_CKM.1/DH_PACE_EAC1P	-	-	-	Х	-	Х
Р						
FCS_CKM.4/EAC1PP	-	-	-	Х	-	Х
FCS_COP.1/PACE_ENC_EAC1P P	-	-	-	Х	-	Х
FCS_COP.1/PACE_MAC_EAC1 PP	-	-	-	Х	-	Х
FCS_RND.1/EAC1PP	-	-	-	Х	-	Х
FCS_CKM.1/CA_EAC1PP	-	-	-	Х	-	Х
FCS_COP.1/CA_ENC_EAC1PP	-	-	-	Х	-	Х
FCS_COP.1/SIG_VER_EAC1PP	-	-	-	Х	-	Х
FCS_COP.1/CA_MAC_EAC1PP	-	-	-	Х	-	Х
FCS_CKM.1/CA2	-	-	-	Х	-	Х
FCS_CKM.1/RI	-	-	-	Х	-	Х
FCS_CKM.1/AA	-	-	-	Х	-	Х
FCS_COP.1/AA	-	-	-	Х	-	Х
FCS_CKM.1/CAM	-	-	-	Х	-	Х
FCS_COP.1/CAM	-	-	-	Х	-	Х
FCS_CKM.1/SSCDPP	-	-	-	Х	-	Х
FCS_COP.1/SSCDPP	-	-	-	Х	-	Х
FIA_AFL.1/Suspend_PIN_EAC2 PP	Х	Х	-	-	-	-
FIA_AFL.1/Block_PIN_EAC2PP	Х	Х	-	-	-	-
FIA_API.1/CA_EAC2PP	-	Х	-	Х	-	Х
FIA_API.1/RI_EAC2PP	-	Х	-	Х	-	Х
FIA_UID.1/PACE_EAC2PP	Х	Х	-	-	-	Х
FIA_UID.1/EAC2_Terminal_EAC 2PP	Х	Х	-	-	-	Х
FIA_UAU.1/PACE_EAC2PP	Х	Х	-	-	-	Х
FIA_UAU.1/EAC2_Terminal_EA C2PP	Х	Х	-	-	-	Х
FIA_UAU.4/PACE_EAC2PP	-	Х	-	-	-	Х
FIA_UAU.5/PACE_EAC2PP	-	Х	-	-	-	Х
FIA_UAU.6/CA_EAC2PP	-	Х	-	-	-	Х
FIA_AFL.1/PACE_EAC2PP	Х	Х	-	-	-	-



TOE SFR / Security Function					uß	
			ent		TSF.AppletParametersSign	
	_		TSF.SecureManagement		ters	
	<u>l</u>	Ð	age		nel	
	on	cat	ana	Ň	rar	
	sc	ntio	eM	ž	Ба	Ę
	es	he	, ni	bte	olet	Į
	ACC ACC	Aut	Sec	S.	Apk	Jat
	<b>FSF.AccessControl</b>	<b>TSF.A</b> uthenticate	Ц. V,	TSF.CryptoKey	Ë.	rSF.Platform
	TS	L S	TS	L S	TS	TS
FIA_UAU.6/PACE_EAC2PP	-	Х	-	-	-	Х
FIA_UID.1/PACE_EAC1PP	Х	Х	-	-	-	Х
FIA_UAU.1/PACE_EAC1PP	Х	Х	-	-	-	Х
FIA_UAU.4/PACE_EAC1PP	-	Х	-	-	-	Х
FIA_UAU.5/PACE_EAC1PP	-	Х	-	-	-	Х
FIA_UAU.6/PACE_EAC1PP	-	X	-	-	-	X
FIA_UAU.6/EAC_EAC1PP	-	Х	-	-	-	X
FIA_API.1/EAC1PP	-	Х	-	X	-	X
FIA_API.1/PACE_CAM	-	X	-	X	-	X
FIA_API.1/AA	- 	X	-	Х	-	Х
FIA_AFL.1/PACE_EAC1PP	X	Х	-	-	-	-
FIA_UID.1/SSCDPP	X	- 	-	-	-	-
FIA_AFL.1/SSCDPP	X X	<u> </u>	-	-	-	-
FIA_UAU.1/SSCDPP	X X	-	-	-	-	-
FDP_ACC.1/TRM_EAC2PP	X X	- X	-	-	-	-
FDP_ACF.1/TRM FDP_RIP.1/EAC2PP		-	-	- X	-	- X
FDP_UCT.1/TRM_EAC2PP	-	-	-	<u>х</u>	-	<u>х</u>
FDP_UIT.1/TRM_EAC2PP	-			<u>х</u>		× X
FDP_ACC.1/TRM_EAC1PP	X	-	-	-	-	-
FDP RIP.1/EAC1PP	-	-		X		X
FDP_UCT.1/TRM_EAC1PP	-	-	-	X	-	X
FDP_UIT.1/TRM_EAC1PP	-	-	-	X	-	X
FDP_ACC.1/SCD/SVD_Generati	Х	-	-	-	-	-
on_SSCDPP	~					
FDP_ACF.1/SCD/SVD_Generati	Х	Х	-	-	-	-
on_SSCDPP						
FDP_ACC.1/SVD_Transfer_SSC DPP	Х	-	-	-	-	-
FDP_ACF.1/SVD_Transfer_SSC DPP	Х	Х	-	-	-	-
FDP_ACC.1/Signature-	Х	_	_	_		_
creation_SSCDPP			-	-	-	-
FDP_ACF.1/Signature- creation_SSCDPP	Х	Х	-	-	-	-
FDP_RIP.1/SSCDPP	-	-	-	Х	-	Х
FDP_SDI.2/Persistent_SSCDPP	-	-	-	-	-	X
FDP_SDI.2/DTBS_SSCDPP	-	-	-	-	-	Х
FTP_ITC.1/PACE_EAC2PP	-	Х	-	Х	-	-
FTP_ITC.1/CA_EAC2PP	-	Х	-	Х	-	-
FTP_ITC.1/PACE_EAC1PP	-	Х	-	Х	-	-
FAU_SAS.1/EAC2PP	-	-	-	-	-	Х
FAU_SAS.1/EAC1PP	-	-	-	-	-	Х
FAU_SAS.I/EACIFF						



TOE SFR / Security Function					dß	
			TSF.SecureManagement		TSF.AppletParametersSign	
	0		gem		etei	
	<b>FSF.AccessControl</b>	TSF.Authenticate	Inaç	>	am	
	ပို့	ıtic	Ma	¥.	Par	ε
	es	her	nre	pto	olet	for
	Acc	Aut	Sec	Sry .	App	lat
	Э.F. /	Э́Е. /	Ц.	ISF.CryptoKey	Э́Е. /	TSF.Platform
				Ц	Ϋ́	L T
FMT_MTD.1/CVCA_UPD_EAC2 PP	Х	Х	Х	-	-	-
FT FMT_SMF.1/EAC2PP	-	-	Х	-	-	Х
FMT_SMR.1	Х	-	-	-	-	X
FMT MTD.1/DATE EAC2PP	Х	Х	Х	-	-	-
FMT_MTD.1/PA_EAC2PP	Х	Х	Х	-	-	-
FMT_MTD.1/SK_PICC_EAC2PP	Х	Х	Х	-	-	-
FMT_MTD.1/KEY_READ_EAC2P	Х	-	Х	-	-	-
Р						
FMT_MTD.1/Initialize_PIN_EAC 2PP	-	Х	Х	-	-	-
FMT_MTD.1/Change_PIN_EAC2 PP	-	Х	Х	-	-	-
FMT_MTD.1/Resume_PIN_EAC2	-	Х	Х	-	-	-
PP FMT_MTD.1/Unblock_PIN_EAC	-	Х	Х	-	-	-
2PP						
FMT_MTD.1/Activate_PIN_EAC2	-	Х	Х	-	-	-
PP FMT MTD.3/EAC2PP		Х				
FMT_SMR.1/SSCDPP	X	-	-	-	-	-
FMT_SMF.1/SSCDPP	-	X	X		-	-
FMT_MOF.1/SSCDPP	Х	X X	X X			-
FMT_MSA.1/Admin_SSCDPP	X	X	X	-	-	-
FMT_MSA.1/SignatorySSCDPP	X	X	X	-	-	-
FMT_MSA.2/SSCDPP	-	-	Х	-	-	-
FMT_MSA.3/SSCDPP	Х	Х	X	-	-	-
FMT_MSA.4/SSCDPP	-	Х	Х	-	-	-
FMT_MTD.1/Admin_SSCDPP	Х	Х	Х	-	-	-
FMT_MTD.1/Signatory_SSCDPP	Х	Х	Х	-	-	-
FMT_LIM.1/EAC2PP	-	-	-	-	-	Х
FMT_LIM.2/EAC2PP	-	-	-	-	-	Х
FMT_MTD.1/INI_ENA_EAC2PP	-	-	-	-	-	Х
FMT_MTD.1/INI_DIS_EAC2PP	-	-	-	-	-	Х
FMT_SMF.1/EAC1PP	-	-	Х	-	-	X
FMT_LIM.1/EAC1PP	-	-	-	-	-	X
FMT_LIM.2/EAC1PP	-	-	-	-	-	X
FMT_MTD.1/INI_ENA_EAC1PP	-	-	-	-	-	X
FMT_MTD.1/INI_DIS_EAC1PP	- V	- V	- V	-	-	Х
FMT_MTD.1/CVCA_INI_EAC1PP FMT_MTD.1/CVCA_UPD_EAC1	X X	X X	X X	-	-	-
PMT_MTD.1/CVCA_OPD_EACT	^	^	^	-		-
FMT_MTD.1/DATE_EAC1PP	Х	Х	Х	-	-	-
FMT_MTD.1/CAPK_EAC1PP	Х	Х	Х	-	-	-



TOE SFR / Security Function	TSF.AccessControl	TSF.Authenticate	TSF.SecureManagement	TSF.CryptoKey	TSF.AppletParametersSign	TSF.Platform
FMT_MTD.1/PA_EAC1PP	Х	Х	Х	-	-	-
FMT_MTD.1/KEY_READ_EAC1P P	Х	-	Х	-	-	-
FMT_MTD.3/EAC1PP	-	Х	-	-	-	-
FMT_LIM.1/Loader	-	-	-	-	-	Х
FMT_LIM.2/Loader	-	-	-	-	-	Х
FMT_MTD.1/AA_Private_Key	Х	Х	Х	-	-	-
FPT_EMS.1/EAC2PP	-	-	-	-	-	Х
FPT_FLS.1/EAC2PP	-	-	-	-	-	Х
FPT_TST.1/EAC2PP	-	-	-	-	Х	Х
FPT_PHP.3/EAC2PP	-	-	-	-	-	Х
FPT_TST.1/EAC1PP	-	-	-	-	Х	Х
FPT_FLS.1/EAC1PP	-	-	-	-	-	Х
FPT_PHP.3/EAC1PP	-	-	-	-	-	Х
FPT_EMS.1/EAC1PP	-	-	-	-	-	Х
FPT_EMS.1/SSCDPP	-	-	-	-	-	Х
FPT_FLS.1/SSCDPP	-	-	-	-	-	Х
FPT_PHP.1/SSCDPP	-	-	-	-	-	Х
FPT_PHP.3/SSCDPP	-	-	-	-	-	Х
FPT_TST.1/SSCDPP	-	-	-	-	Х	Х

## 3874 **7.4.Correspondence of SFR and TOE mechanisms**

3875 Each TOE security functional requirement is implemented by at least one TOE mechanism. In
3876 section 7.1 the implementing of the TOE security functional requirement is described in form
3877 of the TOE mechanism.



## 3878 8. GLOSSARY AND ABBREVIATIONS

3879 For Glossary and Acronyms please refer to the corresponding section of [20].



#### 3880 9. BIBLIOGRAPHY

- [1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- [2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- [3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
- [4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB- 2017-04-004, Version 3.1, Revision 5, April 2017
- [5] BSI: Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012 v1.3.2 (5. December 2012)
- [6] BSI: Common Criteria Protection Profile ID-Card implementing Extended Access Control 2 as defined in BSI TR-03110, BSI-CC-PP-0086-2015 v1.01 (May 20th, 2015)
- [7] ICAO: Technical Report: Supplemental Access Control for Machine Readable Travel Documents, Version - 1.01, 11. November 2010.
- [8] ICAO: ICAO Doc 9303, Part 1: Machine Readable Passports, Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability, Sixth Edition – 2006
- [9] ICAO: ICAO Doc 9303 Machine Readable Travel Documents, 7th edition, 2015
- [10] Inside Secure, Infineon Technologies AG, NXP Semiconductors Germany GmbH, STMicroelectronics: Common Criteria Protection Profile - Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, v1.0 (13.01.2014)
- [11] ISO/IEC 14443 Identification cards Contactless integrated circuit cards,
- [12] ISO/IEC 7816-4:2013 Identification cards Integrated circuit cards Part 4: Organization, security and commands for interchange,
- [13] BSI: Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011
- [14] EN 419211-2:2013 Protection profiles for secure signature creation device Part 2: Device with key generation
- [15] EN 419211-4:2013 Protection profiles for secure signature creation device Part 4: Extension for device with key generation and trusted channel to certificate generation application
- [16] BSI: TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents. Part 1 - eMRTDs with BAC/PACEv2 and EACv1, v2.10 (20. March 2012)



- [17] BSI: TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token. Part 2 – Protocols for electronic IDentification, Authentication and trust Services (eIDAS) Version 2.21, 21. December 2016
- [18] BSI: TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token. Part 3 - Common Specifications v2.21 (21. December 2016)
- [19] BSI: TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token. Part 4 – Applications and Document Profiles V2.21, 21. December 2016
- [20] BSI: Common Criteria Protection Profile Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP], BSI-CC-PP-0087 version 1.01, May 20<sup>th</sup>, 2015
- [21] IDentity Applet Suite v3.4 Administrator's Guide
- [22] IDentity Applet Suite v3.4 User's Guide
- [23] JCOP 4 P71 4 Security Target Lite for JCOP 4 P71 / SE050 Rev. 3.7 2020-03-17
- [24] JCOP 4 P71 D321 User guidance and administrator manual Rev. 3.7 20190531
- [25] Supporting Document Mandatory Technical Document Composite product evaluation for Smart Cards and similar devices; Version 1.5.1, May 2018
- [26] BSI: TR 03111: Elliptic Curve Cryptography, Version 2.0, 28. June 2012.
- [27] RSA Laboratories: PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
- [28] National Institute of Standards and Technology: FIPS PUB 180-4: Secure hash standard, March 2012.
- [29] Published by Oracle. Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., May 2015.
- [30] European card for e-Services and National e-ID applications, IAS ECC European Citizen Card, Technical Specifications, Revisions 1.0.1.
- [31] Bundesamt f
  ür Sicherheit in der Informationstechnik, Technische Richtlinie -Kryptographische Verfahren: Empfehlungen und Schl
  üssell
  ängen, 09. Januar 2013, BSI-TR02102.
- [32] Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication, version 1.0, March 8,2016, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan
- [33] Protection Profile for ePassport IC with SAC (PACE) and Active Authentication, version 1.0, March 8,2016, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan



[34] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library – Security Target Lite – Rev 1.3 – 8 January 2020