

ID&TRUST

IDENTITY APPLET V3.4-P2/EIDAS

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

SECURITY TARGET

COMMON CRITERIA / ISO 15408

EAL4+

2022

Classification: Public

© 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
V1.03	13.05.2022	Updated TOE identification data, TOE name, ST Title, TOE Description and Bibliography.
V1.04	19.07.2022	Update Bibliography and Platform's Certification IDs.
v1.05	19.09.2022	Update Bibliography and Platform's Certification IDs.
v1.06	01.02.2023	Update Bibliography and TOE Reference

Table of Contents

1	1.	ST INTRODUCTION	8
2	1.1.	ST REFERENCE	8
3	1.2.	TOE Reference	8
4	1.3.	TOE Overview.....	9
5	1.3.1.	TOE TYPE.....	9
6	1.3.2.	TOE DEFINITION AND OPERATIONAL USAGE.....	11
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.	TOE 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.	CONFORMANCE CLAIMS	33
16	2.1.	CC Conformance Claim	33
17	2.2.	PP Claim.....	33
18	2.3.	Package Claim.....	35
19	2.4.	Conformance Rationale.....	36
20	2.5.	Statement 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.	Analysis.....	54

27	3.	SECURITY PROBLEM DEFINITION.....	55
28	3.1.	Introduction	55
29	3.1.1.	ASSETS.....	55
30	3.1.2.	SUBJECTS	57
31	3.2.	Threats.....	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.	Organizational 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.	Assumptions	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.	SECURITY OBJECTIVES	66
48	4.1.	Security 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.	Security 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.	Security Objective Rationale	71
61	5.	EXTENDED COMPONENTS DEFINITION	75
62	6.	SECURITY REQUIREMENTS	76
63	6.1.	Security 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.	Security Assurance Requirements for the TOE	165
72	6.3.	Security 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 SUMMARY SPECIFICATION	173
78	7.1.	TOE 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.....	180
84	7.1.6. TSF.Platform.....	180
85	7.2. Assurance Measures.....	183
86	7.3. Fulfillment of the SFRs	183
87	7.4. Correspondence of SFR and TOE mechanisms.....	187
88	8. GLOSSARY AND ABBREVIATIONS	188
89	9. BIBLIOGRAPHY	189
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	10
93	Table 3 Terminals and access control in European Passport	22
94	Table 4 Terminals and access control in Identity Card with Protected MRTD Application.....	26
95	Table 5 Terminals and access control in Identity Card with EU-compliant MRTD Application	
96	30
97	Table 6 Classification of Platform-TSFs.....	39
98	Table 7 Mapping of security objectives for the TOE.....	43
99	Table 8 Mapping of Security requirements	53
100	Table 9 Security Objective Rationale.....	72
101	Table 10 Overview of authentication and identification SFRs	96
102	Table 11 Coverage of Security Objectives for the TOE by SFRs	167
103	Table 12 Assurance measures and corresponding documents.....	183

104 1. ST INTRODUCTION

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

108 1.1. ST REFERENCE

109 Title: Security Target ID&Trust IDentity Applet v3.4-p2/eIDAS - Electronic
110 Identity Card with PACE-GM, PACE-CAM, Extended Access
111 Control v1 and v2, Restricted Identification and Active
112 Authentication

113 Author: ID&Trust Ltd.

114 Version Number: v1.06

115 Date: 01.02.2023

116 1.2. TOE Reference

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

119 TOE Name: IDentity Applet v3.4-p2/eIDAS on NXP JCOP 4 P71

120 TOE short name: IDentity Applet v3.4/eIDAS

121 TOE Identification

122 Data:

123 Applet version
124 number IDentity Applet V3.4/eIDAS v3.4.7470

125 Patch version
126 number: 024A

127 Evaluation Criteria: [4]

128 Evaluation

129 Assurance Level: EAL EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and
130 AVA_VAN.5 as defined in [3].

131 Developer: ID&Trust Ltd.
 132 Evaluation Sponsor: NXP Semiconductors Germany GmbH, Tropelwitzstraße 20, 22529
 133 Hamburg, Germany

134 **1.3.TOE Overview**

135 This ST claims strict conformance to [5], [6], [13] and [20]. There, slightly different terminology
 136 is used. For the ease of understanding, Table 1 gives a brief translation for the used
 137 terminology. Compound words that contain terminology of the table should be replaced
 138 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

139 **Table 1 Overview of identifiers of current ST and PPs**

140 **1.3.1. TOE TYPE**

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

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

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

Table 2 IDentity Applet Suite v3.4 functionalities

144

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

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

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

155 1.3.2. TOE DEFINITION AND OPERATIONAL USAGE

156 The Target of Evaluation (TOE) is a smartcard programmed according to [16] [17]. The
157 smartcard contains multiple applications (at least one). The programmed smartcard is called
158 an electronic document as a whole. Here, an application is a collection of data(groups) and
159 their access conditions. We mainly distinguish between common user data, and sensitive user-
160 data. Depending on the protection mechanisms involved, these user data can further be
161 distinguished as follows:

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

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

168 Due to migration periods, some developers have to implement products that function-ally
169 support both PACE and Basic Access Control (BAC), i.e. Supplemental Access Control (SAC)
170 [8]. However, any product using BAC is not conformant to the current ST; i.e. the TOE may
171 functionally support BAC, but, while performing BAC, it is acting outside of the security policy
172 defined by the current ST.

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

176 Application considered in [16] and [17] are

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

180 The TOE shall comprise at least:

- 181 1. the circuitry of the chip, including all integrated circuit (IC) dedicated software that is
182 active in the operational phase of the TOE,
- 183 2. the IC embedded software, i.e. the operating system,
- 184 3. all access mechanisms, associated protocols and corresponding data,
- 185 4. one or several applications, and
- 186 5. the associated guidance documentation.

187 [2. Application note \(taken from \[20\], application note 2\)](#)

188 Since contactless interface parts (e.g. the antenna) may impact specific aspects of vulnerability
189 assessment and are thus relevant for security, such parts might be considered as a part of the
190 TOE. The decision upon this is up to the certification body in charge that defines the evaluation
191 methodology for the assessment of the contactless interface.

192 [1.3.3. TOE MAJOR SECURITY FEATURES FOR OPERATIONAL USE](#)

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

194 The TOE ensures that

- 195 • only authenticated terminals can get access to the User Data stored on the TOE and
196 use security functionality of the electronic document according to the access rights of
197 the terminal,
- 198 • the Electronic Document Holder can control access by consciously presenting his
199 electronic document and/or by entering his secret PIN,
- 200 • authenticity and integrity of user data can be verified,
- 201 • confidentiality of user data in the communication channel between the TOE and the
202 connected terminal is provided,
- 203 • inconspicuous tracing of the electronic document is averted,
- 204 • its security functionality and the data stored inside are self-protected, and
- 205 • digital signatures can be created, if the TOE contains an eSign application.
- 206 • Optionally support the Active Authentication and Chip Authentication mapping.

207 [1.3.4. NON-TOE HARDWARE/SOFTWARE/FIRMWARE](#)

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

212 [PACE terminal](#)

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

217 For more information see: PACE Terminal

218 [EAC1 terminal](#)

219 An EAC1 terminal is an extended inspection system according to [16]. It performs the
 220 advanced inspection procedure ([16]) using EAC1, i.e. PACE, then Chip Authentication 1
 221 followed by Passive Authentication, and finally Terminal Authentication 1. Afterwards user data
 222 are read by the terminal. An EAC1 terminal is allowed to read both EAC1 protected data, and
 223 common user data.

224 For more information see: [EAC1 Terminal / EAC2 Terminal](#)

225 [EAC2 terminal](#)

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

231 For more information see: [EAC1 Terminal / EAC2 Terminal](#)

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

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

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

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

247 [European Passport configuration](#)

Terminal/Application	ePassport	eID	eSign
----------------------	-----------	-----	-------

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

248 *Identity Card with Protected MRTD Application configuration*

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

249 *Identity Card with EU-compliant MRTD Application configuration*

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

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

253 **1.4. TOE DESCRIPTION**

254 **1.4.1. PRODUCT TYPE**

255 The TOE type addressed by the current ST is a smartcard programmed according to [16] and
 256 [17]. The smartcard contains IDentity Applet v3.4/eIDAS, which may be contain multiple
 257 applications (at least one). The smartcard with IDentity Applet v3.4/eIDAS is called an
 258 electronic document as a whole.

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

261 The TOE type defined both in [5] and [6] is a smartcard. Whereas [5] references [16] (and also
 262 [8] and related ICAO specifications, however [16] is fully compatible with those ICAO
 263 specifications, and they are mostly listed there for the sake of completeness and the context
 264 of use) w.r.t. programming of the card, [17] is given as a reference in [6]. Reference [16] defines
 265 the EAC1 protocol, whereas EAC2 is defined in [17]. Thus, this difference in reference is

266 introduced just due to different applications on the card, that do not contradict each other. The
267 term 'travel document' of [5] is here understood in a more broader sense (cf. also Table 1),
268 since the document can also be used in contexts other than just traveling.

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

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

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

287 1.4.2. COMPONENTS OF THE TOE

288 **Micro Controller**

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

296 **IC dedicated software – Micro Controller Firmware**

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

300 **IC dedicated software – Crypto Library**

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

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

308 Evaluation level EAL6+ ALC_FLR.1 and ASE_TSS.2 according to Security IC Platform
309 Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-00084-
310 2014.

311 **IC Embedded Software**

312 Certification ID: CC-22-180212/2

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

315 OS Name: JCOP 4 Operating System

316 Applied OS
317 configuration: Banking & Secure ID

318
319 Product
320 Identification: JCOP 4 v4.7 R1.01.4

321
322 Evaluation Level: CC EAL 6+ with ASE_TSS.2, ALC_FLR.1 according to Java Card
323 System – Open Configuration Protection Profile, version 3.0.5, Certified
324 by Bundesamt für Sicherheit in der Informationstechnik (BSI, BSI-CC-
325 PP-0099-2017).

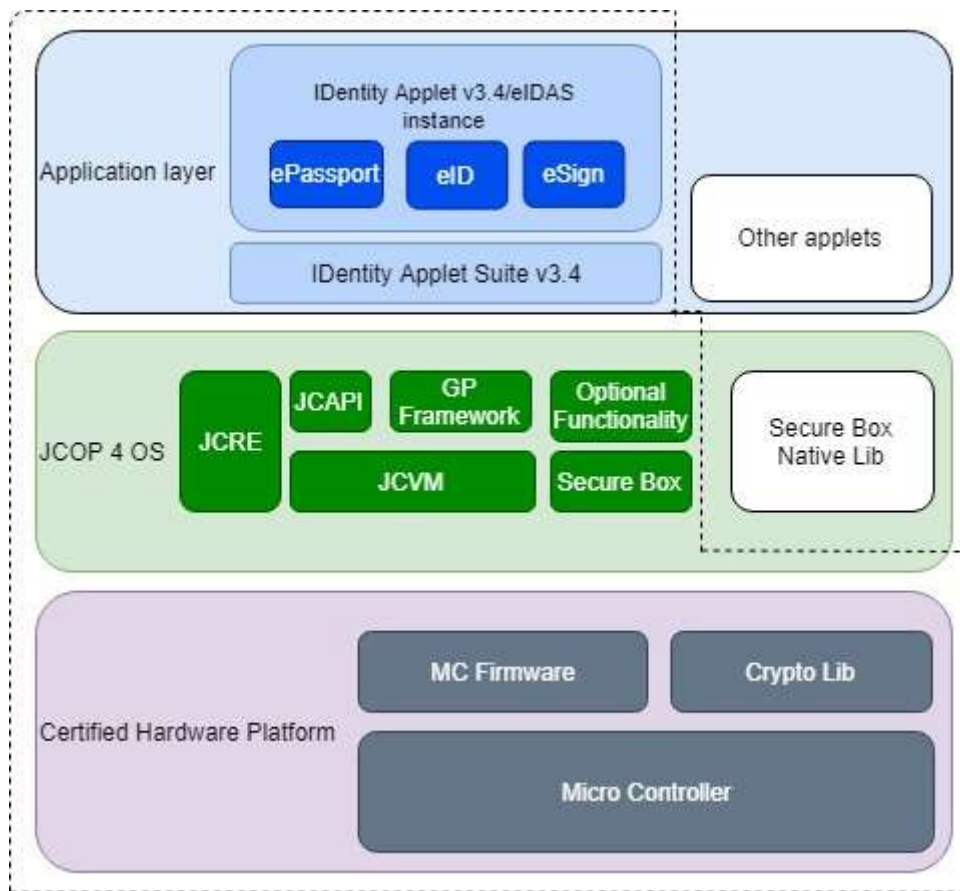
326 Platform UGD: [24]

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

328 Product name: ID&Trust IDentity Applet Suite

329 Version: 3.4

- 330 Application name¹: IDentity Applet v3.4/eIDAS
- 331 TOE Guidance
- 332 Documentation: ² IDentity Applet Administrator’s Guide [21]
- 333 IDentity Applet User’s Guide [22]
- 334 The composite part always means IDentity Applet v3.4/eIDAS
- 335 The logical architecture of the TOE:



336

337

1. Figure TOE Boundaries

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

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

¹ The applet is provided in cap file format.

² The AGD documents provided in electronic document format.

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

345 The boxes marked with white are not certified.

346 1.4.3. TOE LIFE CYCLE

347 The TOE life cycle is described in terms of the above mentioned four life cycle phases. Akin to
348 [10], the TOE life-cycle is additionally subdivided into seven steps.

349 **Phase 1: Development**

350 *Step 1*

351 The TOE is developed in phase 1. NXP develops the integrated circuit, the IC dedicated
352 software and the guidance documentation associated with these TOE components.

353 *Step 2*

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

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

364 **Phase 2: Manufacturing**

365 *Step 3*

366 In a first step, the TOE integrated circuit is produced. The circuit contains the electronic
367 document's chip dedicated software, and the parts of the electronic document's chip
368 embedded software in the non-volatile non-programmable memory (ROM). The IC
369 manufacturer writes IC identification data onto the chip in order to track and control the IC as
370 dedicated electronic document material during IC manufacturing, and during delivery to the

371 electronic document manufacturer. The IC is securely delivered from the IC manufacturer to
372 the electronic document manufacturer. If necessary, the IC manufacturer adds parts of the IC
373 embedded software in the non-volatile programmable memory, e. g. EEPROM or in FLASH.

374 *Step 4 (optional)*

375 If the electronic document manufacturer delivers a packaged component, the IC is combined
376 with hardware for the contact based or contactless interface.

377 *Step 5*

378 The electronic document manufacturer

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

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

386 The pre-personalized electronic document together with the IC identifier is securely delivered
387 from the electronic document manufacturer to the Personalization Agent. The electronic
388 document manufacturer also provides the relevant parts of the guidance documentation to the
389 Personalization Agent.

390 **Phase 3: Personalization of the Electronic Document**

391 *Step 6*

392 The personalization of the electronic document includes

- 393 1. the survey of the Electronic Document Holder's biographical data,
- 394 2. the enrollment of the Electronic Document Holder's biometric reference data, such as
395 a digitized portrait or other biometric reference data,
- 396 3. printing the visual readable data onto the physical part of the electronic document, and
- 397 4. configuration of the TSF, if necessary.

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

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

404 TSF data are data for the operation of the TOE upon which the enforcement of the SFRs relies
 405 [1]. Here TSF data include, but are not limited to, the Personalization Agent's authentication
 406 key(s).

407 **Phase 4: Operational Use**

408 *Step 7*

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

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

413 This ST considers at least the first phase and parts of the second phase, i.e. Step 1 up to Step
 414 3, as part of the evaluation. Therefore, the TOE delivery is defined to occur, according to CC,
 415 after Step 3. Since specific production steps of the second phase are of minor security
 416 relevance (e.g. plastic card or booklet manufacturing and antenna integration) these are not
 417 part of the CC evaluation under ALC. Nevertheless, the decision about this has to be taken by
 418 the certification body resp. the national body of the issuer or organization. In this case the
 419 national body of the issuer is responsible for these specific production steps.

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

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

427 **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.

428 **1.4.5. FEATURES OF THE IDENTITY APPLLET**

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

- 430 • European Passport
- 431 • Identity Card with Protected MRTD Application
- 432 • Identity Card with EU-compliant MRTD Application

433 **1.4.5.1. European Passport**

434 Passwords

- 435 • MRZ [16]
- 436 • CAN [16]

437 Authentication Procedure

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

- 440 • Advanced Inspection procedure [16]

441 Applications

- 442 • ePassport Application

443 Protocols

- 444 • PACE (Generic Mapping, Integrated Mapping and Chip Authentication Mapping) [9],
445 [16]
- 446 • Active Authentication [7] (optionally)
- 447 • EAC1 [16]

448 ○ Terminal Authentication version 1 [16]

449 ○ Chip Authentication version 1 [16]

450 Data Groups

451 According to [16].

452 Data types in:

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

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

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

457 Terminals and access control

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

458 [Table 3 Terminals and access control in European Passport](#)

459 Security Functional Requirements

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

FIA_AFL.1/Block_PIN_EAC2PP	X
FIA_API.1/CA_EAC2PP	-
FIA_API.1/RI_EAC2PP	-
FIA_UID.1/PACE_EAC2PP	-
FIA_UID.1/EAC2_Terminal_EAC2PP	-
FIA_UAU.1/PACE_EAC2PP	-
FIA_UAU.1/EAC2_Terminal_EAC2PP	-
FIA_UAU.4/PACE_EAC2PP	-
FIA_UAU.5/PACE_EAC2PP	-
FIA_UAU.6/CA_EAC2PP	-
FIA_AFL.1/PACE_EAC2PP	-
FIA_UAU.6/PACE_EAC2PP	-
FIA_UID.1/PACE_EAC1PP	X
FIA_UAU.1/PACE_EAC1PP	X
FIA_UAU.4/PACE_EAC1PP	X
FIA_UAU.5/PACE_EAC1PP	X
FIA_UAU.6/PACE_EAC1PP	X
FIA_UAU.6/EAC_EAC1PP	X
FIA_API.1/EAC1PP	X
FIA_API.1/PACE_CAM	X
FIA_API.1/AA	X
FIA_AFL.1/PACE_EAC1PP	X
FIA_UID.1/SSCDPP	-
FIA_AFL.1/SSCDPP	-
FIA_UAU.1/SSCDPP	-
FDP_ACC.1/TRM_EAC2PP	-
FDP_ACF.1/TRM	X
FDP_RIP.1/EAC2PP	-
FDP_UCT.1/TRM_EAC2PP	-
FDP_UIT.1/TRM_EAC2PP	-
FDP_ACC.1/TRM_EAC1PP	X
FDP_RIP.1/EAC1PP	X
FDP_UCT.1/TRM_EAC1PP	X
FDP_UIT.1/TRM_EAC1PP	X
FDP_ACC.1/SCD/SVD_Generation_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	X
FAU_SAS.1/EAC2PP	-
FAU_SAS.1/EAC1PP	X
FMT_MTD.1/CVCA_INI_EAC2PP	-
FMT_MTD.1/CVCA_UPD_EAC2PP	-
FMT_SMF.1/EAC2PP	-

FMT_SMR.1	X
FMT_MTD.1/DATE_EAC2PP	-
FMT_MTD.1/PA_EAC2PP	-
FMT_MTD.1/SK_PICC_EAC2PP	-
FMT_MTD.1/KEY_READ_EAC2PP	-
FMT_MTD.1/Initialize_PIN_EAC2PP	-
FMT_MTD.1/Change_PIN_EAC2PP	-
FMT_MTD.1/Resume_PIN_EAC2PP	-
FMT_MTD.1/Unblock_PIN_EAC2PP	-
FMT_MTD.1/Activate_PIN_EAC2PP	-
FMT_MTD.3/EAC2PP	-
FMT_SMR.1/SSCDPP	-
FMT_SMF.1/SSCDPP	-
FMT_MOF.1/SSCDPP	-
FMT_MSA.1/Admin_SSCDPP	-
FMT_MSA.1/SignatorySSCDPP	-
FMT_MSA.2/SSCDPP	-
FMT_MSA.3/SSCDPP	-
FMT_MSA.4/SSCDPP	-
FMT_MTD.1/Admin_SSCDPP	-
FMT_MTD.1/Signatory_SSCDPP	-
FMT_LIM.1/EAC2PP	-
FMT_LIM.2/EAC2PP	-
FMT_MTD.1/INI_ENA_EAC2PP	-
FMT_MTD.1/INI_DIS_EAC2PP	-
FMT_SMF.1/EAC1PP	X
FMT_LIM.1/EAC1PP	X
FMT_LIM.2/EAC1PP	X
FMT_MTD.1/INI_ENA_EAC1PP	X
FMT_MTD.1/INI_DIS_EAC1PP	X
FMT_MTD.1/CVCA_INI_EAC1PP	X
FMT_MTD.1/CVCA_UPD_EAC1PP	X
FMT_MTD.1/DATE_EAC1PP	X
FMT_MTD.1/CAPK_EAC1PP	X
FMT_MTD.1/PA_EAC1PP	X
FMT_MTD.1/KEY_READ_EAC1PP	X
FMT_MTD.3/EAC1PP	X
FMT_LIM.1/Loader	X
FMT_LIM.2/Loader	X
FMT_MTD.1/AA_Private_Key	X
FPT_EMS.1/EAC2PP	-
FPT_FLS.1/EAC2PP	-
FPT_TST.1/EAC2PP	-
FPT_PHP.3/EAC2PP	-
FPT_TST.1/EAC1PP	X
FPT_FLS.1/EAC1PP	X
FPT_PHP.3/EAC1PP	X
FPT_EMS.1/EAC1PP	X
FPT_EMS.1/SSCDPP	-
FPT_FLS.1/SSCDPP	-
FPT_PHP.1/SSCDPP	-
FPT_PHP.3/SSCDPP	-
FPT_TST.1/SSCDPP	-

460 **1.4.5.2. Identity Card with Protected MRTD Application**

461 Passwords

462 • MRZ [16]

463 • CAN [16]

464 • PIN [17]

465 • PUK [17]

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

470 **Authentication Procedure**

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

473 • General Authentication Procedure [17]

474 Applications

475 • ePassport Application

476 • eID Application

477 • eSign Application

478 **Protocols**

479 • PACE (Generic Mapping, Integrated Mapping) [17]

480 • EAC2 [17]

481 ○ Terminal Authentication version 2 [17]

482 ○ Chip Authentication version 2 [17]

483 • Restricted Identification [17]

484 Data Groups

485 According to [17].

486 According to [9] and [16].

487 Data type in:

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

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

491 Terminals and access control

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

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

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

FIA_UAU.6/PACE_EAC1PP	-	-	-
FIA_UAU.6/EAC_EAC1PP	-	-	-
FIA_API.1/EAC1PP	-	-	-
FIA_API.1/PACE_CAM	-	-	-
FIA_API.1/AA	-	-	-
FIA_AFL.1/PACE_EAC1PP	-	-	-
FIA_UID.1/SSCDPP	-	-	X
FIA_AFL.1/SSCDPP	-	-	X
FIA_UAU.1/SSCDPP	-	-	X
FDP_ACC.1/TRM_EAC2PP	X	X	X
FDP_ACF.1/TRM	X	X	X
FDP_RIP.1/EAC2PP	X	X	X
FDP_UCT.1/TRM_EAC2PP	X	X	X
FDP_UIT.1/TRM_EAC2PP	X	X	X
FDP_ACC.1/TRM_EAC1PP	-	-	-
FDP_RIP.1/EAC1PP	-	-	-
FDP_UCT.1/TRM_EAC1PP	-	-	-
FDP_UIT.1/TRM_EAC1PP	-	-	-
FDP_ACC.1/SCD/SVD_Generation_SSCDPP	-	-	X
FDP_ACF.1/SCD/SVD_Generation_SSCDPP	-	-	X
FDP_ACC.1/SVD_Transfer_SSCDPP	-	-	X
FDP_ACF.1/SVD_Transfer_SSCDPP	-	-	X
FDP_ACC.1/Signature-creation_SSCDPP	-	-	X
FDP_ACF.1/Signature-creation_SSCDPP	-	-	X
FDP_RIP.1/SSCDPP	-	-	X
FDP_SDI.2/Persistent_SSCDPP	-	-	X
FDP_SDI.2/DTBS_SSCDPP	-	-	X
FTP_ITC.1/PACE_EAC2PP	X	X	X
FTP_ITC.1/CA_EAC2PP	X	X	X
FTP_ITC.1/PACE_EAC1PP	-	-	-
FAU_SAS.1/EAC2PP	X	X	X
FAU_SAS.1/EAC1PP	-	-	-
FMT_MTD.1/CVCA_INI_EAC2PP	X	X	X
FMT_MTD.1/CVCA_UPD_EAC2PP	X	X	X
FMT_SMF.1/EAC2PP	X	X	-
FMT_SMR.1	X	X	X
FMT_MTD.1/DATE_EAC2PP	X	X	X
FMT_MTD.1/PA_EAC2PP	X	X	X
FMT_MTD.1/SK_PICC_EAC2PP	X	X	X
FMT_MTD.1/KEY_READ_EAC2PP	X	X	-
FMT_MTD.1/Initialize_PIN_EAC2PP	X	X	-
FMT_MTD.1/Change_PIN_EAC2PP	X	X	
FMT_MTD.1/Resume_PIN_EAC2PP	X	X	
FMT_MTD.1/Unblock_PIN_EAC2PP	X	X	
FMT_MTD.1/Activate_PIN_EAC2PP	X	X	
FMT_MTD.3/EAC2PP	X	X	
FMT_SMR.1/SSCDPP	-	-	X
FMT_SMF.1/SSCDPP	-	-	X
FMT_MOF.1/SSCDPP	-	-	X
FMT_MSA.1/Admin_SSCDPP	-	-	X
FMT_MSA.1/SignatorySSCDPP	-	-	X
FMT_MSA.2/SSCDPP	-	-	X

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

493 **1.4.5.3. Identity Card with EU-compliant MRTD Application**

494 Passwords

- 495 • MRZ [16]
- 496 • CAN [16]
- 497 • PIN [17]
- 498 • PUK [17]

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

503 Authentication Procedure

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

- 506 • Advanced Inspection Procedure [16]

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

- 509 • General Authentication Procedure [17]

510 Applications

- 511 • ePassport Application

- 512 • eID Application

- 513 • eSign Application

514 Protocols

- 515 • PACE (Generic Mapping, Integrated Mapping and Chip Authentication Mapping) [9]
516 [16] and [17]

- 517 • Active Authentication [7] (optionally)

- 518 • EAC1 [16]

- 519 ○ Terminal Authentication version 1 [16]

- 520 ○ Chip Authentication version 1 [16]

- 521 • EAC2 [17]

- 522 ○ Terminal Authentication version 2 [17]

- 523 ○ Chip Authentication version 2 [17]

- 524 • Restricted Identification [17]

525 Data Groups

526 According to [17].

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

- 529 • Common user data: All DG, which require only BAC/PACE protocol in ePassport;

- 530 • EAC1 protected data: All DG, which require EAC1 protocol in ePassport;

- 531 • EAC2 protected data: All DG in eID and eSign application.

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

534 Terminals and access control

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

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

536

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

FIA_UAU.4/PACE_EAC2PP	-	X	X
FIA_UAU.5/PACE_EAC2PP	-	X	X
FIA_UAU.6/CA_EAC2PP	-	X	X
FIA_AFL.1/PACE_EAC2PP	-	X	X
FIA_UAU.6/PACE_EAC2PP	-	X	X
FIA_UID.1/PACE_EAC1PP	X	-	-
FIA_UAU.1/PACE_EAC1PP	X	-	-
FIA_UAU.4/PACE_EAC1PP	X	-	-
FIA_UAU.5/PACE_EAC1PP	X	-	-
FIA_UAU.6/PACE_EAC1PP	X	-	-
FIA_UAU.6/EAC_EAC1PP	X	-	-
FIA_API.1/EAC1PP	X	-	-
FIA_API.1/PACE_CAM	X	-	-
FIA_API.1/AA	X	-	-
FIA_AFL.1/PACE_EAC1PP	X	-	-
FIA_UID.1/SSCDPP	-	-	X
FIA_AFL.1/SSCDPP	-	-	X
FIA_UAU.1/SSCDPP	-	-	X
FDP_ACC.1/TRM_EAC2PP	-	X	X
FDP_ACF.1/TRM	X	X	X
FDP_RIP.1/EAC2PP	-	X	X
FDP_UCT.1/TRM_EAC2PP	-	X	X
FDP_UIT.1/TRM_EAC2PP	-	X	X
FDP_ACC.1/TRM_EAC1PP	X	-	-
FDP_RIP.1/EAC1PP	X	-	-
FDP_UCT.1/TRM_EAC1PP	X	-	-
FDP_UIT.1/TRM_EAC1PP	X	-	-
FDP_ACC.1/SCD/SVD_Generation_SSCDPP	-	-	X
FDP_ACF.1/SCD/SVD_Generation_SSCDPP	-	-	X
FDP_ACC.1/SVD_Transfer_SSCDPP	-	-	X
FDP_ACF.1/SVD_Transfer_SSCDPP	-	-	X
FDP_ACC.1/Signature-creation_SSCDPP	-	-	X
FDP_ACF.1/Signature-creation_SSCDPP	-	-	X
FDP_RIP.1/SSCDPP	-	-	X
FDP_SDI.2/Persistent_SSCDPP	-	-	X
FDP_SDI.2/DTBS_SSCDPP	-	-	X
FTP_ITC.1/PACE_EAC2PP	-	X	X
FTP_ITC.1/CA_EAC2PP	-	X	X
FTP_ITC.1/PACE_EAC1PP	X	-	-
FAU_SAS.1/EAC2PP	-	X	X
FAU_SAS.1/EAC1PP	X	-	-
FMT_MTD.1/CVCA_INI_EAC2PP	-	X	X
FMT_MTD.1/CVCA_UPD_EAC2PP	-	X	X
FMT_SMF.1/EAC2PP	-	X	-
FMT_SMR.1	X	X	X
FMT_MTD.1/DATE_EAC2PP	-	X	X
FMT_MTD.1/PA_EAC2PP	-	X	X
FMT_MTD.1/SK_PICC_EAC2PP	-	X	X
FMT_MTD.1/KEY_READ_EAC2PP	-	X	-
FMT_MTD.1/Initialize_PIN_EAC2PP	-	X	-
FMT_MTD.1/Change_PIN_EAC2PP	-	X	-
FMT_MTD.1/Resume_PIN_EAC2PP	-	X	-

FMT_MTD.1/Unblock_PIN_EAC2PP	-	X	
FMT_MTD.1/Activate_PIN_EAC2PP	-	X	
FMT_MTD.3/EAC2PP	-	X	
FMT_SMR.1/SSCDPP	-	-	X
FMT_SMF.1/SSCDPP	-	-	X
FMT_MOF.1/SSCDPP	-	-	X
FMT_MSA.1/Admin_SSCDPP	-	-	X
FMT_MSA.1/SignatorySSCDPP	-	-	X
FMT_MSA.2/SSCDPP	-	-	X
FMT_MSA.3/SSCDPP	-	-	X
FMT_MSA.4/SSCDPP	-	-	X
FMT_MTD.1/Admin_SSCDPP	-	-	X
FMT_MTD.1/Signatory_SSCDPP	-	-	X
FMT_LIM.1/EAC2PP	-	X	X
FMT_LIM.2/EAC2PP	-	X	X
FMT_MTD.1/INI_ENA_EAC2PP	-	X	X
FMT_MTD.1/INI_DIS_EAC2PP	-	X	X
FMT_SMF.1/EAC1PP	X	-	-
FMT_LIM.1/EAC1PP	X	-	-
FMT_LIM.2/EAC1PP	X	-	-
FMT_MTD.1/INI_ENA_EAC1PP	X	-	-
FMT_MTD.1/INI_DIS_EAC1PP	X	-	-
FMT_MTD.1/CVCA_INI_EAC1PP	X	-	-
FMT_MTD.1/CVCA_UPD_EAC1PP	X	-	-
FMT_MTD.1/DATE_EAC1PP	X	-	-
FMT_MTD.1/CAPK_EAC1PP	X	-	-
FMT_MTD.1/PA_EAC1PP	X	-	-
FMT_MTD.1/KEY_READ_EAC1PP	X	-	-
FMT_MTD.3/EAC1PP	-	-	-
FMT_LIM.1/Loader	X	X	X
FMT_LIM.2/Loader	X	X	X
FMT_MTD.1/AA_Private_Key	X	-	-
FPT_EMS.1/EAC2PP	-	X	X
FPT_FLS.1/EAC2PP	-	X	X
FPT_TST.1/EAC2PP	-	X	X
FPT_PHP.3/EAC2PP	-	X	X
FPT_TST.1/EAC1PP	X	-	
FPT_FLS.1/EAC1PP	X	-	
FPT_PHP.3/EAC1PP	X	-	
FPT_EMS.1/EAC1PP	X	-	
FPT_EMS.1/SSCDPP	-	-	X
FPT_FLS.1/SSCDPP	-	-	X
FPT_PHP.1/SSCDPP	-	-	X
FPT_PHP.3/SSCDPP	-	-	X
FPT_TST.1/SSCDPP	-	-	X

537 [5. Application note \(from the ST author\)](#)

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

543 **2. CONFORMANCE CLAIMS**544 **2.1.CC Conformance Claim**

545 This ST claims conformance to

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

552 as follows

553 Part 2 extended,

554 Part 3 conformant.

555 The

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

558 has to be taken into account.

559 **2.2.PP Claim**560 This ST claims **strict conformance** to the following protection profile:

561 **Title:** **Machine-Readable Electronic Documents based on BSI TR-03110**
562 **for Official Use [MR.ED-PP] [20]**

563 **Sponsor:** Bundesamt für Sicherheit in der Informationstechnik (BSI)

564 **CC version:** 3.1 (Revision 3.4)

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

566 **General Status:** Final

567 **Version number:** 1.01

568 **Registration:** BSI-CC-PP-0087

569 Keywords: ICAO, PACE, EAC, Extended Access Control, ID-Card, electronic
570 document, smart card, TR-03110
571

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

574 **Title:** **Machine Readable Travel Document with „ICAO Application”,**
575 **Extended Access Control with PACE (EAC PP) [5]**

576 Sponsor: Bundesamt für Sicherheit in der Informationstechnik
577 CC Version: 3.1 (revision 3)
578 Assurance Level: EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
579 General Status: Final
580 Version number: version 1.3.2
581 Registration: BSI-CC-PP-0056-V2-2012
582 Keywords: ICAO, Machine Readable Travel Document, Extended Access Control,
583 PACE, Supplemental Access Control (SAC)
584

585 **Title:** **Common Criteria Protection Profile Electronic Document**
586 **implementing Extended Access Control Version 2 defined in BSI**
587 **TR-03110 [6]**

588 Editor/Sponsor: Bundesamt für Sicherheit in der Informationstechnik (BSI)
589 CC Version: 3.1 (Revision 4)
590 Assurance Level: EAL4 augmented ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.
591 General Status: final
592 Version Number: Version 1.01
593 Registration: BSI-CC-PP-0086
594 Keywords: EAC2, eID-Application, eID-Card, PACE
595

596 **Title:** **Protection profiles for Secure signature creation device — Part 2:**
597 **Device with key generation**

598 Author: CEN / CENELEC (TC224/WG17)
599 CC Version: 3.1 (Revision 3)
600 Assurance Level: EAL4 augmented with AVA_VAN.5
601 Version Number: Version 2.0.1

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

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

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

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

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

613 **Title: Machine Readable Travel Document using Standard Inspection**
614 **Procedure with PACE (PACE PP) [13]**

615 Sponsor: Bundesamt für Sicherheit in der Informationstechnik

616 CC Version: 3.1 (revision 4)

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

618 General Status: Final

619 Version number: Version 1.01

620 Registration: BSI-CC-PP-0068-V2-2011-MA-01

621 Keywords: ePassport, travel document, ICAO, PACE, Standard Inspection
622 Procedure, Supplemental Access Control (SAC)

623

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

628 **2.3.Package Claim**

629 The current ST is conformant to the following packages:

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

632 **2.4.Conformance Rationale**

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

634 1. The TOE type of this ST is the same as the TOE type of the claimed PPs:

635 The Target of Evaluation (TOE) is an electronic document implemented as a smart
636 card programmed according to [16] and [17], and additionally representing a
637 combination of hardware and software configured to securely create, use and manage
638 signature-creation data , for the eSign application.

639 2. The security problem definition (SPD) of this ST contains the SPD of the claimed PPs.
640 The SPD contains all threats, organizational security policies and assumptions of the
641 claimed PPs.

642 The current ST extended the OSP **P.Terminal** because of the optional Active
643 Authentication function of TOE.

644 3. The security objectives for the TOE in this ST include all the security objectives for the
645 TOE of the claimed PPs. This objective does not weaken the security objectives of the
646 claimed PPs.

647 In addition, the OT.Chip_Auth_Proof_PACE_CAM security objective is defined in the
648 ST because of the Chip Authentication mapping and OT.Chip_Auth_Proof_AA
649 because of the Active Authentication protocol.

650 4. The security objectives for the operational environment in this ST include all security
651 objectives for the operational environment of the claimed PPs.

652 In addition the OE.Auth_Key_AA and OE.Exam_Electronic_Document_AA security
653 objectives are defined in the ST because of the Active Authentication protocol. These
654 additions were necessary because none of the original security objectives for the TOE
655 or OSPs do not concern the obligations of States or Organization in connection with
656 Active Authentication protocol.

657 5. Those SFR, which are refined in order to ensure the unified terminology usage, are not
658 detailed in the following.

659 The SFRs specified in this ST include all security functional requirements (SFRs)
660 specified in the claimed PPs. We especially point to the following three refined SFRs
661 within [20]:

662 The SFR FIA_UAU.1/SSCDPP is redefined from [14] by additional assignments. Note
663 that this does not violate strict conformance to [14].

664 Multiple iterations of FDP_ACF.1 and FMT_SMR.1 exist from imported PPs to define
665 the access control SFPs and security roles for (common) user data, EAC1-protected

666 user data, and EAC2-protected user data. These access control SFPs and security
667 roles are unified to FDP_ACF.1/TRM and FMT_SMR.1.

668 The following SFRs were iterated from FCS_CKM.1, FCS_COP.1 and FIA_API.1 to
669 the ST because of PACE-CAM:

- 670 • FCS_CKM.1/CAM
- 671 • FCS_COP.1/CAM
- 672 • FIA_API.1/PACE_CAM

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

- 674 • FPT_EMS.1/EAC1PP

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

- 676 • FIA_UID.1/PACE_EAC1PP
- 677 • FIA_UAU.5/PACE_EAC1PP

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

- 680 • FCS_CKM.1/AA
- 681 • FCS_COP.1/AA
- 682 • FIA_API.1/AA
- 683 • FMT_MTD.1/AA_Private_Key

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

- 685 • FIA_UAU.1/PACE_EAC1PP
- 686 • FPT_EMS.1/EAC1PP

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

- 688 • FIA_UAU.4/PACE_EAC1PP
- 689 • FMT_MTD.1/KEY_READ_EAC1PP

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

- 694 • FCS_CKM.1/CA2
- 695 • FCS_CKM.1/RI

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

- 698 • FMT_MTD.1/SK_PICC_EAC2PP

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

701 • FDP_RIP.1/EAC2PP

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

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

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

709 **2.5.Statement of Compatibility**

710 **2.5.1. SECURITY FUNCTIONALITIES**

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

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

Platform Security Functionality	Corresponding TOE Security Functionality	Relevant or not relevant	Remarks
SF.JCVM	TSF.Platform	Relevant	Java Card Virtual Machine
SF.CONFIG	TSF.Platform	Relevant	Configuration Management
SF.OPEN	TSF.AccessControl TSF.Authenticate TSF.Platform	Relevant	Card Content Management
SF.CRYPTO	TSF.AppletParametersSi gn TSF.Authenticate TSF.CryptoKey TSF.Platform	Relevant	Cryptographic Functionality
SF.RNG	TSF.CryptoKey TSF.Platform	Relevant	Random Number Generator
SF.DATA_STORAGE	TSF.AccessControl TSF.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.AppletParametersSign TSF.Authenticate	Relevant	PIN Management
SF.PERS_MEM	TSF.Platform	Relevant	Persistent Memory Management
SF.SENS_RES	-	Not relevant	Sensitive Result
SF.EDC	TSF.Platform	Relevant	Error Detection Code API
SF.HW_EXC	TSF.Platform	Relevant	Hardware Exception Handling
SF.RM	-	Not relevant	Restricted Mode
SF.PID	-	Not relevant	Platform Identification
SF.SMG_NSC	TSF.Platform	Relevant	No Side-Channel
SF.ACC_SBX	-	Not relevant	Secure Box
SF.MOD_INVOC	-	Not relevant	Module Invocation

Table 6 Classification of Platform-TSFs

716

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

718 **2.5.2. OSPs**

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

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

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

727 **2.5.3. SECURITY OBJECTIVES**

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

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

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

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

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

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

730 **Table 7 Mapping of security objectives for the TOE**

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

- 733 • **OT.SID**
- 734 • **OT.APPLI-AUTH**
- 735 • **OT.ATTACK-COUNTER**
- 736 • **OT.EXT-MEM**
- 737 • **OT.FIREWALL**
- 738 • **OT.Global_ARRAYS_INTEG**
- 739 • **OT.NATIVE**
- 740 • **OT.OBJ-DELETION**
- 741 • **OT.RESTRICTED-MODE**
- 742 • **OT.SEC_BOX_FW**
- 743 • **OT.SENSITIVE_RESULT_INTEG**

744 cannot be mapped because these are out of scope.

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

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

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

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

747 **2.5.4. SECURITY REQUIREMENTS**

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

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
FAU_ARP.1	FPT_PHP.3/EAC2PP FPT_PHP.3/EAC1PP FPT_PHP.3/SSCDPP	RP_SFR-MECH	FAU_ARP.1 facilitate to protect the TOE as required by these SFRs./SSCD
FAU_SAS.1[SCP]	FAU_SAS.1/EAC2PP FAU_SAS.1/EAC1PP	RP_SFR-MECH	FAU_SAS.1[SCP] covers these SFRs.
FCO_NRO.2[SC]	-	IP_SFR	-
FCS_CKM.1t	-	IP_SFR	-
FCS_COP.1	FCS_CKM.1/DH_PACE_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[ECDHPACEKeyAgreement] is applied for key agreement during the PACE-CAM.
	FCS_CKM.1/CA2	RP_SFR-SERV	FCS_CKM.1.1 is applied for generation chip authentication key(s) pair on the TOE:
	FCS_CKM.1/RI	RP_SFR-SERV	FCS_CKM.1.1 is applied for generation chip restricted identification key pair(s) on the TOE:
	FCS_CKM.1/AA	RP_SFR-SERV	FCS_CKM.1.1 is applied for generation chip active authentication key pair on the TOE:
	FCS_CKM.1/SSCDPP	RP_SFR-SERV	FCS_CKM.1.1 is applied for generation chip SCD/SVD key pair on the TOE:
	FCS_COP.1/PACE_ENC_EAC2PP	RP_SFR-SERV	FCS_COP1.1[AES] is applied for nonce encryption during the PACE protocol. FCS_COP1.1[AES] is applied for encryption and decryption during secure messaging (PACE)
	FCS_COP.1/PACE_ENC_EAC1PP	RP_SFR-SERV	FCS_COP1.1[AES] or FCS_COP.1[TripleDES] is applied for nonce encryption during the PACE-CAM protocol. FCS_COP1.1[AES] or FCS_COP.1[TripleDES] is applied for encryption and decryption during secure messaging (PACE).
	FCS_COP.1/SHA_EAC2PP	RP_SFR-SERV	FCS_COP1.1[SHA] is applied for session key derivation during CA2 and ephemeral key compression (CA2 and TA2).
	FCS_COP.1/CAM	RP_SFR-SERV	FCS_COP.1.1[AES] is applied for message encryption of Chip Authentication Data.
	FCS_CKM.1/CA_EAC1PP	RP_SFR-SERV	FCS_COP.1.1[ECDHPACEKeyAgreement] is applied for key agreement related to CA1 FCS_COP1.1[SHA] is applied for session key derivation during CA1.
	FCS_COP.1/SIG_VER_EAC2PP	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] orFCS_COP.1.1[ECSignature]

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

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
			<p>message authentication codes.</p> <p>FCS_COP1.1[AESMAC] is applied during secure messaging to verify the message authentication codes.</p> <p>FCS_COP1.1[SHA] is applied for public key compression (in case DH).</p>
	FIA_UAU.5/PACE_EAC1 PP	RP_SFR-SERV	<p>FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during PACE secure messaging the verify the message authentication codes.</p> <p>FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during CA secure messaging to verify the message authentication codes.</p> <p>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.</p> <p>FCS_COP1.1[SHA] is applied for public key compression (in case DH).</p>
	FIA_UAU.6/PACE_EAC2 PP FIA_UAU.6/PACE_EAC1 PP	RP_SFR-SERV	<p>FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during PACE secure messaging the verify the message authentication codes</p>
	FIA_UAU.6/EAC_EAC1P P	RP_SFR-SERV	<p>FCS_COP.1.1[AESMAC] o FCS_COP.1[DESMAC] is applied for message authentication code generation and verification related to PACE.</p>
	FIA_UAU.6/CA_EAC2PP	RP_SFR-SERV	<p>FCS_COP.1.1[AESMAC] is applied for message authentication code generation and verification related to CA2.</p>
	FIA_UAU.6/EAC_EAC1P P	RP_SFR-SERV	<p>FCS_COP.1.1[AESMAC] o FCS_COP.1[DESMAC] is applied for message authentication code</p>

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
			generation and verification related to CA1.
	FIA_API.1/EAC1PP	RP_SFR-SERV	FCS_COP1.1[AESMAC] is applied for message authentication code verification related to CA1.
	FIA_API.1/AA	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] or FCS_COP.1.1[ECSignature] is applied for digital signature verification for Active Authentication protocol..
	FIA_API.1/PACE_CAM	RP_SFR-SERV	FCS_COP.1.1[AESMAC] is applied for chip authentication data generation related to PACE-CAM.
	FDP_UCT.1/TRM_EAC1P P	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] or FCS_COP.1.1[ECSignature] is applied for digital signature verification for TA.
	FDP_UIT.1/TRM_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[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	RP_SFR-SERV	FCS_COP.1[TripleDES] or FCS_COP.1[AES] and FCS_COP.1[DESMAC] or FCS_COP.1[AESMAC] are applied during secure messaging to protect against disclosure and modification
	FMT_MTD.3/EAC2PP FMT_MTD.3/EAC1PP	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] or FCS_COP.1.1[ECSSignature] is applied for digital signature verification for TA1 and TA2.
FCS_RNG.1	FCS_RND.1/EAC2PP	RP_SFR-SERV	FCS_RNG.1 provides nonce and challenge generation for PACE and TA2.
	FCS_RND.1/EAC1PP	RP_SFR-SERV	FCS_COP.1[TripleDES] or FCS_COP.1[AES] is applied during secure messaging to protect the confidentiality of transmitted and received user data.
	FIA_UAU.4/PACE_EAC2PP	RP_SFR-SERV	FCS_RNG.1 is applied to generate fresh nonce for PACE and TA2
	FIA_UAU.4/PACE_EAC1PP	RP_SFR-SERV	FCS_RNG.1 is applied to generate fresh nonce for PACE, TA1 and Active Authentication.
	FDP_UCT.1/TRM_EAC2P	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	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[ADEL]	-	IP_SFR	
FDP_ACC.2[RM]	-	IP_SFR	-
FDP_ACC.1[EXT-MEM]	-	IP_SFR	
FDP_ACF.1[EXT-MEM]	-	IP_SFR	-
FDP_ACC.2[SecureBox]	-	IP_SFR	
FDP_ACF.1[SecureBox]	-	IP_SFR	
FDP_ACF.1[RM]	-	IP_SFR	-
FDP_IFC.1[JCVML]	-	IP_SFR	-
FDP_IFC.2[SC]	-	IP_SFR	-
FDP_IFC.2[CFG]	FMT_LIM.1/Loader FMT_LIM.2/Loader FMT_LIM.1/EAC2PP FMT_LIM.2/EAC2PP FMT_LIM.1/EAC1PP FMT_LIM.2/EAC1PP	RP_SFR-MECH	FDP_IFC.2[CFG] applied to protect the TOE in operational phase.
FDP_IFC.1[MODULAR-DESIGN]	-	IP_SFR	
FDP_IFF.1[JCVML]	-	IP_SFR	-
FDP_IFF.1[SC]	FMT_MTD.1/INI_ENA_EAC2PP FMT_MTD.1/INI_DIS_EAC2PP FMT_MTD.1/INI_ENA_EA1PP FMT_MTD.1/INI_DIS_EAC1PP	RP_SFR-MECH	FDP_IFF.1[SC] applied to control the writing of initialization and pre-personalization data as required by these SFRs.
FDP_IFF.1[CFG]	-	IP_SFR	-
FDP_IFF.1[MODULAR-DESIGN]	-	IP_SFR	-
FDP_ITC.2[CCM]	-	IP_SFR	-
FDP_RIP.1[OBJECTS]	-	IP_SFR	-
FDP_RIP.1[ABORT]	-	IP_SFR	-
FDP_RIP.1[APDU]	-	IP_SFR	-
FDP_RIP.1[bArray]	-	IP_SFR	-
FDP_RIP.1[GlobalArray_Refined]	-	IP_SFR	-
FDP_RIP.1[KEYS]	FDP_RIP.1/EAC2PP FDP_RIP.1/EAC1PP FDP_RIP.1/SSCDPP	RP_SFR-MECH	FDP_RIP.1[KEYS] is applied to destroy the secure message session keys, the PACE

Platform SFR	Corresponding TOE SFR	Category of Platform's SFRs	Remarks
			ephemeral private key and SCD.
FDP_RIP.1[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 ULAR-DESIGN]	-	IP_SFR	-
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_Termin al_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	-
FMT_MSA.1[JCR E]	-	IP_SFR	-
FMT_MSA.1[JCV M]	-	IP_SFR	-
FMT_MSA.1[AD EL]	-	IP_SFR	-
FMT_MSA.1[SC]	-	IP_SFR	-
FMT_MSA.1[EXT -MEM]	-	IP_SFR	-
FMT_MSA.1[SecureBox]	-	IP_SFR	-
FMT_MSA.1[CFG]	-	IP_SFR	-
FMT_MSA.1[SD]	-	IP_SFR	-
FMT_MSA.1[RM]	-	IP_SFR	-
FMT_MSA.1[MODULAR-DESIGN]	-	IP_SFR	-
FMT_MSA.2[FIREWALL-JCVM]	-	IP_SFR	-
FMT_MSA.3[FIREWALL]	-	IP_SFR	-
FMT_MSA.3[JCV M]	-	IP_SFR	-
FMT_MSA.3[AD EL]	-	IP_SFR	-
FMT_MSA.3[EXT -MEM]	-	IP_SFR	-
FMT_MSA.3[SecureBox]	-	IP_SFR	-
FMT_MSA.3[CFG]	-	IP_SFR	-
FMT_MSA.3[SD]	-	IP_SFR	-
FMT_MSA.3[SC]	-	IP_SFR	-
FMT_MSA.3[RM]	-	IP_SFR	-
FMT_MSA.3[MODULAR-DESIGN]	-	IP_SFR	-
FMT_MTD.1[JCR E]	-	IP_SFR	-
FMT_MTD.3[JCR E]	-	IP_SFR	-
FMT_SMF.1	-	IP_SFR	-
FMT_SMF.1[AD EL]	-	IP_SFR	-
FMT_SMF.1[EXT -MEM]	-	IP_SFR	-
FMT_SMF.1[SecureBox]	-	IP_SFR	-

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

Table 8 Mapping of Security requirements

749

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

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

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

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

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

763

764 **2.5.5. ASSURANCE REQUIREMENTS**

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

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

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

771 **2.6.Analysis**

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

773 3. SECURITY PROBLEM DEFINITION

774 3.1.Introduction

775 3.1.1. ASSETS

776 3.1.1.1.Primary Assets

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

779 **Authenticity of the Electronic Document's Chip**

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

783 *Generic Security Property: Authenticity*

784 This asset is equal to the one(s) of [5] and [6], which itself stem from [13].

785 **Electronic Document Tracing Data**

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

789 *Generic Security Property: Unavailability*

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

792 **Sensitive User Data**

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

796 *Generic Security Properties: Confidentiality, Integrity, Authenticity*

797 User Data stored on the TOE

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

802 *Generic Security Properties: Confidentiality, Integrity, Authenticity*

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

806 User Data transferred between the TOE and the Terminal

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

810 *Generic Security Properties: Confidentiality, Integrity, Authenticity*

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

816 *3.1.1.2.Secondary Assets*

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

819 Accessibility to the TOE Functions and Data only for Authorized Subjects

820 Property of the TOE to restrict access to TSF and TSF-Data stored in the TOE to authorized
821 subjects only.

822 *Generic Security Property: Availability*

823 Genuineness of the TOE

824 Property of the TOE to be authentic in order to provide claimed security functionality in a proper
825 way.

826 *Generic Security Property: Availability*

827 **Electronic Document Communication Establishment Authorization Data**

828 Restricted-revealable authorization information for a human user being used for verification of
829 the authorization attempts as an authorized user (PACE password). These data are stored in
830 the TOE and are not send to it.

831 Restricted-revealable here refers to the fact that if necessary, the Electronic Document Holder
832 may reveal her verification values of CAN and MRZ to an authorized person, or to a device
833 that acts according to respective regulations and is considered trustworthy.

834 *Generic Security Properties: Confidentiality, Integrity*

835 **Secret Electronic Document Holder Authentication Data**

836 Secret authentication information for the Electronic Document Holder being used for
837 verification of the authentication attempts as authorized Electronic Document Holder (PACE
838 passwords).

839 *Generic Security Properties: Confidentiality, Integrity*

840 **TOE internal Non-Secret Cryptographic Material**

841 Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret
842 material used by the TOE in order to enforce its security functionality.

843 *Generic Security Properties: Integrity, Authenticity*

844 **TOE internal Secret Cryptographic Keys**

845 Permanently or temporarily stored secret cryptographic material used by the TOE in order to
846 enforce its security functionality.

847 *Generic Security Properties: Confidentiality, Integrity*

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

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

850 **3.1.2. SUBJECTS**

851 This ST considers the following external entities and subjects:

852 Attacker

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

857 Country Signing Certification Authority (CSCA)

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

864 Country Verifying Certification Authority (CVCA)

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

870 Document Signer (DS)

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

875 Document Verifier (DV)

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

879 Electronic Document Holder

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

883 Electronic Document Presenter

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

887 Manufacturer

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

893 PACE Terminal

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

899 Personalization Agent

900 An organization acting on behalf of the electronic document issuer that personalizes the
901 electronic document for the Electronic Document Holder. Personalization includes some or all
902 of the following activities:

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

914 the operational policy of the electronic document issuer. This subject includes
915 “Administrator” as defined in [14].

916 **EAC1 Terminal / EAC2 Terminal**

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

922 **Terminal**

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

927 **3.2.Threats**

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

931 **T.InconsistentSec**

932 **Inconsistency of security measures**

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

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

940 Asset: authenticity, integrity and confidentiality of User Data stored on
941 the TOE

942 **T.Interfere**

943 **Interference of security protocols**

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

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

948 Asset: authenticity, integrity and confidentiality of User Data stored on
949 the TOE

950 **3.2.1. THREATS FROM EAC1PP**

951 This ST includes the following threats from [5]. They concern EAC1-protected data.

- 952 • **T.Counterfeit**
- 953 • **T.Read_Sensitive_Data**

954 Due to identical definitions and names they are not repeated here. For the remaining threats
955 from [5], cf. Chapter 3.2.3.

956 **3.2.2. THREATS FROM EAC2PP**

957 This ST includes the following threats from the [6]. They concern EAC2-protected data.

- 958 • **T.Counterfeit/EAC2**
- 959 • **T.Sensitive_Data**

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

961 **3.2.3. THREATS FROM PACEPP**

962 Both [5] and [6] claim [13], and thus include the threats formulated in [13]. We list each threat
963 only once here. Due to identical definitions and names, their definitions are not repeated here.

- 964 • **T.Abuse-Func**
- 965 • **T.Eavesdropping**
- 966 • **T.Forgery**
- 967 • **T.Information_Leakage**
- 968 • **T.Malfunction**
- 969 • **T.Phys-Tamper**
- 970 • **T.Skimming**
- 971 • **T.Tracing**

972 **3.2.4. THREATS FROM SSCDPP**

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

- 975 • **T.DTBS_Forgery**
- 976 • **T.Hack_Phys**
- 977 • **T.SCD_Derive**
- 978 • **T.SCD_Divulge**
- 979 • **T.Sig_Forgery**
- 980 • **T.SigF_Misuse**
- 981 • **T.SVD_Forgery**

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

983 **3.3.Organizational Security Policies**

984 The TOE shall comply with the following Organizational Security Policies (OSP) as security
985 rules, procedures, practices, or guidelines imposed by an organization upon its operations (see
986 [1], sec. 3.2). This ST includes the OSPs from the claimed protection profiles as listed below
987 and provides no further OSPs.

988 **3.3.1. OSPs FROM EAC1PP**

989 This ST includes the following OSPs from [5], if the TOE contains EAC1-protected data.

990 • **P.Personalisation**

991 • **P.Sensitive_Data**

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

994 **3.3.2. OSPs FROM EAC2PP**

995 This ST includes the following OSPs from [6]. They mainly concern EAC2-protected data.

996 • **P.EAC2_Terminal**

997 • **P.RestrictedIdentity**

998 • **P.Terminal_PKI**

999 Due to identical definitions and names, their definitions are not repeated here. For the
1000 remaining OSPs from [6], cf. the next section.

1001 **3.3.3. OSPs FROM PACEPP**

1002 This ST includes the following OSPs from [13], since both [5] and [6] claim [13]. We list each
1003 OSP only once here. Due to identical definitions and names, their definitions are not repeated
1004 here as well.

1005 • **P.Card_PKI**

1006 • **P.Manufact**

1007 • **P.Pre-Operational**

1008 • **P.Trustworthy_PKI**

1009 **3.3.4. OSPs FROM SSCDPP**

1010 The current ST also includes all OSPs of [14]. They are applicable, if the eSign application is
1011 included.

1012 • **P.CSP_QCert**

1013 • **P.QSign**

1014 • **P.Sig_Non-Repud**

1015 • **P.Sigy_SSCD**

1016 Due to identical definitions and names, their definitions are not repeated here.

1017 **3.3.5. ADDITIONAL OSPs**

1018 The next OSP addresses the need of a policy for the document manufacturer. It is formulated
1019 akin to [10].

1020 **P.Lim_Block Loader**

1021 The composite manufacturer uses the Loader for loading of Security IC Embedded Software,
1022 user data of the Composite Product or IC Dedicated Support Software in charge of the IC
1023 Manufacturer. She limits the capability and blocks the availability of the Loader in order to
1024 protect stored data from disclosure and manipulation.

1025 The ST includes the following OSP from [13], since both [5] and [6] claim [13], but the
1026 **P.Terminal** was extended because the Active Authentication protocol. The extension is
1027 marked with **bold** and the other part of the OSP remained unchanged.

1028 **P.Terminal**

1029 The PACE terminal shall operate their terminals as follows:

- 1030 1. The related terminals (PACE terminal) shall be used by terminal operators and by travel
1031 document holders as defined in [9].
- 1032 2. They shall implement the terminal parts of the PACE protocol [9], of the Passive
1033 Authentication [9] and use them in this order³. The PACE terminal shall use randomly and
1034 (almost) uniformly selected nonce, if required by the protocols (for generating ephemeral
1035 keys for Diffie-Hellmann).
1036 **Furthermore the PACE terminal and EAC1 terminal shall implement the terminal parts**
1037 **of the Active Authentication protocol as described in [9].**
- 1038 3. The related terminals need not to use any own credentials.
- 1039 4. They shall also store the Country Signing Public Key and the Document Signer Public Key
1040 (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive
1041 Authentication(determination of the authenticity of data groups stored in the travel
1042 document, [9]).
- 1043 5. The related terminals and their environment shall ensure confidentiality and integrity of
1044 respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI
1045 certificates, etc.), where it is necessary for a secure operation of the TOE according to the
1046 [13].

³ This order is commensurate with [9].

1047 **Justification:** The modification of **P.Terminal** is extended the original OSP in order to support
1048 the Active Authentication protocol. Taking into consideration the extension is not modify the
1049 original OSP, but added further requirements, this extension is not hurt the strict conformance
1050 as determined in PP Claim.

1051 3.4.Assumptions

1052 The assumptions describe the security aspects of the environment in which the TOE will be
1053 used or is intended to be used. This ST includes the assumptions from the claimed protection
1054 profiles as listed below and defines no further assumptions.

1055 3.4.1. ASSUMPTIONS FROM EAC1PP

1056 This ST includes the following assumptions from the [5]. They concern EAC1-protected data.

- 1057 • **A.Auth_PKI**
- 1058 • **A.Insp_Sys**

1059 Due to identical definitions and names, their definitions are not repeated here. For the
1060 remaining assumptions from [5], see the next sections.

1061 3.4.2. ASSUMPTIONS FROM EAC2PP

1062 [6] only includes the assumption from [13] (see below) and defines no other assumption.

1063 3.4.3. ASSUMPTIONS FROM PACEPP

1064 This ST includes the following assumptions from [13], since both [5] and [6] claim [13].

- 1065 • **A.Passive_Auth**

1066 Due to an identical definition and name, its definition is not repeated here as well.

1067 3.4.4. ASSUMPTIONS FROM SSCDPP

1068 The current ST also includes all assumptions of [14]. These items are applicable, if the eSign
1069 application is included.

- 1070 • **A.CGA**
- 1071 • **A.SCA**

1072 Due to identical definitions and names their definitions are not repeated here.

1073 4. SECURITY OBJECTIVES

1074 This chapter describes the security objectives for the TOE and for the TOE environment. The
1075 security objectives for the TOE environment are separated into security objectives for the
1076 development, and production environment and security objectives for the operational
1077 environment.

1078 4.1. Security Objectives for the TOE

1079 This section describes the security objectives for the TOE, addressing the aspects of identified
1080 threats to be countered by the TOE, and organizational security policies to be met by the TOE.

1081 OT.Non_Interfere

1082 No interference of Access Control Mechanisms

1083 The various implemented access control mechanisms must be consistent. Their
1084 implementation must not allow to circumvent an access control mechanism by exploiting an
1085 unintended implementational interference of one access control mechanism with another one.

1086 OT.Chip_Auth_Proof_AA

1087 Proof of the electronic documents authenticity with Active Authentication

1088 The TOE must support the Terminal to verify the identity and authenticity of the electronic
1089 document as issued by the identified issuing State or Organisation by means of the Active
1090 Authentication protocol as defined in [7], [9]. The authenticity proof provided by electronic
1091 document shall be protected against attacks with high attack potential.

1092 4.1.1. SECURITY OBJECTIVES FOR THE TOE FROM EAC1PP

1093 This ST includes the following additional security objectives for the TOE from [5] that are not
1094 included in [13]. They concern EAC1-protected data.

1095 • OT.Chip_Auth_Proof

1096 • OT.Sens_Data_Conf

1097 Due to identical definitions and names, their definitions are not repeated here. For the
1098 remaining security objectives from [5], see the next sections.

1099 In addition, the following security objective is defined here:

1100 **OT.Chip_Auth_Proof_PACE_CAM**

1101 **Proof of the electronic document's chip authenticity**

1102 The TOE must support the terminals to verify the identity and authenticity of the Electronic
1103 document's chip as issued by the identified issuing State or Organization by means of the
1104 PACE-Chip Authentication Mapping (PACE-CAM) as defined in [9]. The authenticity proof
1105 provided by electronic document's chip shall be protected against attacks with high attack
1106 potential.

1107 **Application note 8 (from ST author)**

1108 PACE-CAM enables much faster authentication of the of the chip than running PACE with
1109 General Mapping (according to [16]) followed by CA1. OT.Chip_Auth_Proof_PACE_CAM is
1110 intended to require the Chip to merely provide an additional means – with the same level of
1111 security – of authentication.

1112 **4.1.2. SECURITY OBJECTIVES FOR THE TOE EAC2PP**

1113 This ST includes the following additional security objectives for the TOE from [6] that are not
1114 included in [13]. They concern EAC2-protected data.

- 1115 • **OT.AC_Pers_EAC2**
- 1116 • **OT.CA2**
- 1117 • **OT.RI_EAC2**
- 1118 • **OT.Sens_Data_EAC2**

1119 Due to identical definitions and names, their definitions are not repeated here. For the
1120 remaining security objectives from [6], see the next sections.

1121 **4.1.3. SECURITY OBJECTIVES FOR THE TOE PACEPP**

1122 Both [5] and [6] claim [13]. Therefore, the following security objectives are included as well.
1123 We list them only once here.

- 1124 • **OT.AC_Pers**
- 1125 • **OT.Data_Authenticity**
- 1126 • **OT.Data_Confidentiality**
- 1127 • **OT.Data_Integrity**
- 1128 • **OT.Identification**
- 1129 • **OT.Prot_Abuse-Func**
- 1130 • **OT.Prot_Inf_Leak**
- 1131 • **OT.Prot_Malfunction**
- 1132 • **OT.Prot_Phys-Tamper**
- 1133 • **OT.Tracing**

1134 Due to identical definitions and names, their definitions are not repeated here.

1135 **4.1.4. SECURITY OBJECTIVES FOR THE TOE SSCDPP**

1136 The current ST also includes all security objectives for the TOE of [14]. These items are
1137 applicable, if an eSign application is included.

- 1138 • **OT.DTBS_Integrity_TOE**
- 1139 • **OT.EMSEC_Design**
- 1140 • **OT.Lifecycle_Security**
- 1141 • **OT.SCD_Secrecy**
- 1142 • **OT.SCD_SVD_Corresp**
- 1143 • **OT.SCD_Unique**
- 1144 • **OT.SCD/SVD_Gen**
- 1145 • **OT.Sig_Secure**
- 1146 • **OT.Sigy_SigF**
- 1147 • **OT.Tamper_ID**
- 1148 • **OT.Tamper_Resistance**

1149 Due to identical definitions and names, their definitions are not repeated here as well. Note
1150 that all are formally included here, but careful analysis reveals that OT.SCD_Secrecy,
1151 OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID, and OT.Tamper_Resistance
1152 are actually fully or partly covered by security objectives included from [13].

1153 **4.1.5. ADDITIONAL SECURITY OBJECTIVES FOR THE TOE**

1154 A loader is a part of the chip operating system that allows to load data, i.e. the file-
1155 system/applet containing (sensitive) user data, TSF data etc. into the Flash memory after
1156 delivery of the smartcard to the document manufacturer.

1157 The following objective for the TOE addresses limiting the availability of the loader, and is
1158 formulated akin to [10].

1159 **OT.Cap_Avail Loader**

1160 The TSF provides limited capability of the Loader functionality of the TOE embedded software
1161 and irreversible termination of the Loader in order to protect user data from disclosure and
1162 manipulation.

1163 **4.2.Security Objectives for the Operational Environment**

1164 **4.2.1. SECURITY OBJECTIVES FROM EAC1PP**

1165 This ST includes the following security objectives for the TOE from the [5]. They mainly concern
1166 EAC1-protected data.

- 1167 • **OE.Auth_Key_Travel_Document**
- 1168 • **OE.Authoriz_Sens_Data**
- 1169 • **OE.Exam_Travel_Document**
- 1170 • **OE.Ext_Insp_Systems**
- 1171 • **OE.Prot_Logical_Travel_Document**

1172 Due to identical definitions and names, their definitions are not repeated here. For the
1173 remaining ones, see the next sections

1174 **4.2.2. SECURITY OBJECTIVES FROM EAC2PP**

1175 This ST includes the following security objectives for the TOE from the [6]. They mainly concern
1176 EAC2-protected data.

1177 • **OE.Chip_Auth_Key**

1178 • **OE.RestrictedIdentity**

1179 • **OE.Terminal_Authentication**

1180 Due to identical definitions and names, their definitions are not repeated here. For the
1181 remaining ones, see the next section.

1182 **4.2.3. SECURITY OBJECTIVES FROM PACEPP**

1183 Both [5] and [6] claim [13]. Therefore, the following security objectives on the operational
1184 environment are included as well. We repeat them only once here.

1185 • **OE.Legislative_Compliance**

1186 • **OE.Passive_Auth_Sign**

1187 • **OE.Personalisation**

1188 • **OE.Terminal**

1189 • **OE.Travel_Document_Holder**

1190 Due to identical definitions and names, they are not repeated here as well.

1191 **4.2.4. SECURITY OBJECTIVES FROM SSCDPP**

1192 The current ST also includes all security objectives for the TOE of [14]. These items are
1193 applicable, if an eSign application is included.

1194 • **OE.CGA_QCert**

1195 • **OE.DTBS_Intend**

1196 • **OE.DTBS_Protect**

1197 • **OE.HID_VAD**

1198 • **OE.Signatory**

1199 • **OE.SSCD_Prov_Service**

1200 • **OE.SVD_Auth**

1201 Due to identical definitions and names, their definitions are not repeated here.

1202 **4.2.5. ADDITIONAL SECURITY OBJECTIVES FOR THE ENVIRONMENT**

1203 The following objective on the environment is defined akin to the objective from [10].

1204 **OE.Lim_Block Loader**

1205 The manufacturer will protect the Loader functionality against misuse, limit the capability of the
1206 Loader and terminate irreversibly the Loader after intended usage of the Loader.

1207 **Justification:** This security objective directly addresses the threat **OT.Non_Interfere**. This
1208 threat concerns the potential interference of different access control mechanisms, which could
1209 occur as a result of combining different applications on a smartcard. Such combination does
1210 not occur in one of the claimed PPs. Hence, this security objective for the environment does –
1211 neither mitigate a threat of one of the claimed PPs that was addressed by security objectives
1212 of that PP,– nor does it fulfill any organizational security policy of one of the claimed PPs that
1213 was meant to be addressed by security objectives of the TOE of that PP.

1214 The following objectives on the environment are introduced because of the Active
1215 Authentication

1216 • **OE.Auth_Key_AA**1217 **Electronic document Active Authentication key pair**

1218 The issuing State or Organisation has to establish the necessary infrastructure in order to (i)
1219 generate the electronic document's Active Authentication Key Pair, (ii) sign (Passive
1220 Authentication) and store the Active Authentication Public Key in the Active Authentication
1221 Public Key data in EF.DG15 and (iii) support Terminals of receiving States or Organisations to
1222 verify the authenticity of the electronic document used for genuine electronic document.

1223 • **OE.Exam_Electronic_Document_AA**1224 **Examination of the genuineness of the electronic document with Active Authentication**

1225 The Terminal of the receiving State or Organisation perform the Active Authentication protocol
1226 according to [7] and [9] in order to verify the genuineness of the presented electronic document.

1227 **4.3.Security Objective Rationale**

1228 Table 9 provides an overview of the security objectives' coverage. According to [1], the tracing
1229 between security objectives and the security problem definition must ensure that 1) *each*
1230 *security objective traces to at least one threat, OSP and assumption, 2) each threat, OSP and*
1231 *assumption has at least one security objective tracing to it, and 3) the tracing is correct (i.e.*
1232 *the main point being that security objectives for the TOE do not trace back to assumptions).*

1233 This is illustrated in the following way:

- 1234 1. can be inferred for security objectives from claimed PPs by looking up the security
 1235 objective rationale of the claimed PPs and for newly introduced security objectives
 1236 because of [20] or the newly introduced functions (i.e. **OE.Lim_Block_Loader**,
 1237 **OT.Cap_Avail_Loader**, **OT.Chip_Auth_Proof_AA**, **OE.Auth_Key_AA**,
 1238 **OE.Exam_Electronic_Document_AA** and **OT.Chip_Auth_Proof_PACE_CAM**) by
 1239 checking the columns of Table 9 ,
- 1240 2. can be inferred for threats, OSPs and assumptions from the claimed PPs by looking up
 1241 the security objective rationale of the claimed PPs and for newly introduced or
 1242 extended⁴ threats, OSPs and assumptions by checking the rows of Table 9 , and
- 1243 3. simply by checking the columns of Table 9 and the security objective rationales from
 1244 the claimed PPs.

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

Table 9 Security Objective Rationale

1245

1246 The threat **T.InconsistentSec** addresses attacks on the confidentiality and the integrity of User
 1247 Data stored on the TOE, facilitated by the data not being protected as intended.

1248 OT.AC_Pers and OT.AC_Pers_EAC2 define the restriction on writing or modifying data;

1249 OT.Data_Authenticity, OT.Data_Confidentiality, OT.Data_Integrity, OT.Sens_Data_Conf
 1250 (from [5]), and **OT.Sens_Data_EAC2** require the security of stored user data as well as user
 1251 data that are transferred between the TOE and a terminal to be secure w.r.t. authenticity,
 1252 integrity and confidentiality.

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

1253 OT.Non_Interfere requires the TOE's access control mechanisms to be implemented
1254 consistently and their implementations not to allow to circumvent an access control mechanism
1255 by exploiting an unintended implementational interference of one access control mechanism
1256 with another one. OT.Cap_Avail Loader requires the TOE to provide limited capability of the
1257 loader functionality and irreversible termination of the loader in order to protect stored user
1258 data.

1259 OE.Lim_Block Loader requires the manufacturer to protect the loader functionality against
1260 misuse, limit the capability of the loader, and terminate irreversibly the loader after intended
1261 usage of the loader.

1262 The combination of these security objectives cover the threat posed by **T.InconsistentSec**.

1263 The threat **T.Interfere** addresses the attack on user data by exploiting the unintended
1264 interference of security protocols. This is directly countered by OT.Non_Interfere, requiring the
1265 TOE's access control mechanisms to be implemented consistently, and their implementations
1266 to not allow to circumvent an access control mechanism by exploiting an unintended
1267 implementational interference of one access control mechanism with another one.

1268 The threat **T.Counterfeit** (from [5]) is countered in [5] by OT.Chip_Auth_Proof. That security
1269 objectives addresses the implementation of the Chip Authentication Protocol Version 1 (CA1)
1270 and thus counters the thread of counterfeiting an electronic document containing an ePassport
1271 application. Here, the additional security objective for the TOE
1272 OT.Chip_Auth_Proof_PACE_CAM is introduced. It ensures that the chip in addition to CA1
1273 also supports the PACE-Chip Authentication Mapping (PACE-CAM) protocol, which supports
1274 the same security functionality as CA1 does. PACE-CAM enables much faster authentication
1275 of the of the chip than running PACE with general mapping followed by CA1.

1276 Furthermore **T.Counterfeit** is countered by OT.Chip_Auth_Proof_AA, OE.Auth_Key_AA and
1277 OE.Exam_Electronic_Document_AA. These security objectives addresses the implementation
1278 of the Active Authentication and thus counters the thread of counterfeiting an electronic
1279 document containing an ePassport application. It ensures that the chip supports the Active
1280 Authentication protocol, which supports to verify that the electronic document is genuine
1281 (similar as Chip Authentication without secure messaging).

1282 The OSP **P.Lim_Block Loader** addresses limiting the capability and blocking the availability
1283 of the Loader in order to protect stored data from disclosure and manipulation. This is
1284 addressed by OT.Cap_Avail Loader, which requires the TOE to provide a limited capability of

1285 the loader functionality and irreversible termination of the loader in order to protect stored user
1286 data; by OT.Non_Interfere, which requires the TOE's access control mechanisms to be
1287 implemented consistently and their implementations not to allow to circumvent an access
1288 control mechanism by exploiting an unintended implementational interference of one access
1289 control mechanism with another one; and by OE.Lim_Block Loader, which requires the
1290 manufacturer to protect the Loader functionality against misuse, limit the capability of the
1291 Loader and terminate irreversibly the Loader after intended usage of the Loader.

1292 The OSP **P.Terminal** is extended to support the Active Authentication protocol. With this
1293 extension the **P.Terminal** countered by the security objective
1294 **OE.Exam_Electronic_Document_AA**. The **OE.Exam_Electronic_Document_AA** enforces
1295 the terminal parts of the Active Authentication.

1296 **5. EXTENDED COMPONENTS DEFINITION**

1297 This ST includes all extended components from the claimed PPs. This includes

- 1298 • FAU_SAS.1 from the family FAU_SAS from [13]
- 1299 • FCS_RND.1 from the family FCS_RND from [13]
- 1300 • FMT_LIM.1 and FMT_LIM.2 from the family FMT_LIM [13]
- 1301 • FPT_EMS.1 from the family FPT_EMS from [13]
- 1302 • FIA_API.1 from the family FIA_API from [6]

1303 For precise definitions we refer to [13] and [6].

1304 **6. SECURITY REQUIREMENTS**

1305 This part defines detailed security requirements that shall be satisfied by the TOE. The
1306 statement of TOE security requirements shall define the *functional* and *assurance* security
1307 requirements that the TOE must satisfy in order to meet the security objectives for the TOE.

1308 Common Criteria allows several operations to be performed on security requirements on the
1309 component level: *refinement*, *selection*, *assignment* and *iteration*, cf. sec. 8.1 of [1]. Each of
1310 these operations is used in this ST.

1311 The **refinement** operation is used to add detail to a requirement, and thus further restricts a
1312 requirement. Refinements of security requirements are denoted in such a way that added
1313 words are in **bold text** and removed words are ~~crossed-out~~.

1314 The **selection** operation is used to select one or more options provided by CC in stating a
1315 requirement. Selections that have been made by the PP author are denoted as underlined text.
1316 Selections to be filled in by the ST author appear in square brackets with an indication that a
1317 selection has to be made, [selection:], and are *italicized*. Selections filled in by the ST author
1318 are denoted as double underlined text and a foot note where the selection choices from the
1319 PP are listed.

1320 The **assignment** operation is used to assign a specific value to an unspecified parameter,
1321 such as the length of a password. Assignments that have been made by the PP author are
1322 denoted as underlined text. Assignments to be filled in by the ST author appear in square
1323 brackets with an indication that an assignment has to be made [assignment:], and are *italicized*.
1324 In some cases the assignment made by the PP authors defines a selection to be performed
1325 by the ST author. Thus this text is underlined and italicized *like this*. Assignments filled in by
1326 the ST author are denoted as double underlined text.

1327 The **iteration** operation is used when a component is repeated with varying operations.
1328 Iteration is denoted by showing a slash “/”, and the iteration indicator after the component
1329 identifier. For the sake of better readability, the iteration operation may also be applied to a
1330 non-repeated single component in order to indicate that such component belongs to a certain
1331 functional cluster. In such a case, the iteration operation is applied to only one single
1332 component.

1333 In order to distinguish between SFRs defined here and SFRs that are taken over from PPs to
1334 which this ST claims strict conformance, the latter are iterated resp. renamed in the following
1335 way:

1336 /EAC1PP or /XXX_EAC1PP [5],

1337 /EAC2PP or /XXX_EAC2PP for [6],

1338 and /SSCDPP or /XXX_SSCDPP for [14].

1339 **6.1.Security Functional Requirements**

1340 The statements of security requirements must be internally consistent. As several different PPs
1341 with similar SFRs are claimed, great care must be taken to ensure that these several iterated
1342 SFRs do not lead to inconsistency.

1343 Despite this ST claims strict conformance to [13], SFRs can be safely ignored in this ST as
1344 long as [5] and [6] are taken into account.

1345 One must remember that each of these iterated SFRs mostly concerns different (groups of)
1346 user and TSF data for each protocol (i.e. PACE, EAC1 and EAC2). Three cases are
1347 distinguished:

- 1348 1. The SFRs apply to different data that are accessible by executing different protocols.
1349 Hence, they are completely separate. An example is FCS_CKM.1/DH_PACE from [5]
1350 and [6]. No remark is added in such case in the text below.
- 1351 2. The SFRs are equivalent. Then we list them all for the sake of completeness. Hence,
1352 it suffices to consider only one iteration. For such SFRs, we explicitly give a remark. An
1353 example is FIA_AFL.1/PACE from [5] and [6].
- 1354 3. The SFRs do not apply to different data or protocols, but are also not completely
1355 equivalent. Then these multiple SFRs are refined in such a way, that one common
1356 component is reached that subsumes all iterations that stem from the inclusions of the
1357 claimed PPs. An example is FDP_ACF.1, which is combined here from [5] and [6].
1358 Such a case is also explicitly mentioned in the text.

1359 Thus internal consistency is not violated.

1360 **6.1.1. Class FCS**

1361 The following SFRs are imported due to claiming [6]. They concern cryptographic support for
 1362 applications that contain EAC2-protected data groups.

- 1363 • **FCS_CKM.1/DH_PACE_EAC2PP**
- 1364 • **FCS_COP.1/SHA_EAC2PP**
- 1365 • **FCS_COP.1/SIG_VER_EAC2PP**
- 1366 • **FCS_COP.1/PACE_ENC_EAC2PP**
- 1367 • **FCS_COP.1/PACE_MAC_EAC2PP**
- 1368 • **FCS_CKM.4/EAC2PP**
- 1369 • **FCS_RND.1/EAC2PP**

1370 **FCS_CKM.1/DH_PACE_EAC2PP**
 1371 Cryptographic Key Generation – Diffie-Hellman for PACE and CA2 Session Keys

1372 Hierarchical to: No other components

1373 Dependencies: [FCS_CKM.2 Cryptographic key distribution or
 1374 FCS_COP.1 Cryptographic operation] not fulfilled, but
 1375 **justified:**
 1376 A Diffie-Hellman key agreement is used in order to
 1377 have no key distribution, therefore FCS_CKM.2 makes
 1378 no sense in this case.

1379 FCS_CKM.4 Cryptographic key destruction fulfilled by
 1380 FCS_CKM.4/EAC2PP

1381 **FCS_CKM.1.1/DH_PACE_EAC2PP**

1382 The TSF shall generate cryptographic keys in accordance with a specified cryptographic
 1383 key generation algorithm Diffie-Hellman-Protocol compliant to [27] and ECDH compliant
 1384 to [26]]⁵⁶ and specified cryptographic key sizes AES 128, 192, 256⁷ that meet the following:
 1385 **[17]**⁸

1386 **9. Application note (taken from [6], application note 10)**

⁵ [assignment: *cryptographic key generation algorithm*]
⁶ [selection: *Diffie-Hellman-Protocol compliant to [27] , ECDH compliant to [26]*]
⁷ [assignment: *cryptographic key sizes*]
⁸ [assignment: *list of standards*]

1387 In the above and all subsequent related SFRs, the reference w.r.t. the PACE protocol is
 1388 changed to [17], whereas [13] references [7]. The difference between the two definitions is that
 1389 [17] defines additional optional parameters for the command MSE:Set AT. This optional
 1390 parameters (e.g. the CHAT) are technically required, since here Terminal Authentication 2
 1391 (TA2) can be executed right after PACE (see FIA_UID.1/EAC2_Terminal_EAC2PP). As [7]
 1392 does not consider TA2, no such definition is given there. These additional parameters are
 1393 optional and not used during PACE itself (only afterwards). If PACE is run without TA2
 1394 afterwards, access to data on the chip is given as specified by [13]. If TA2 is run afterwards,
 1395 access to data on the chip can be further restricted w.r.t. to the authorization level of the
 1396 terminal. Therefore, this change of references does not violate strict conformance to [13]. We
 1397 treat this change of references as a refinement operation, and thus mark the changed
 1398 reference using **bold** text.

1399 [10. Application note \(redefined by ST author, taken from \[6\], application note 11\)](#)

1400 Applied.

1401 [11. Application note \(taken from \[6\], application note 12\)](#)

1402 [13] considers Diffie-Hellman key generation only for PACE. Since the TOE is required to
 1403 implement Chip Authentication 2 (cf. FIA_API.1/CA_EAC2PP), here
 1404 FCS_CKM.1/DH_PACE_EAC2PP applies for CA2 as well.

1405 FCS_COP.1/SHA_EAC2PP
 1406 Cryptographic operation – Hash for key derivation

1407 Hierarchical to: No other components

1408 Dependencies: [FDP_ITC.1 Import of user data without security
 1409 attributes, or FDP_ITC.2 Import of user data with
 1410 security attributes, or FCS_CKM.1 Cryptographic key
 1411 generation] not fulfilled, but **justified**:
 1412 A hash function does not use any cryptographic key;
 1413 hence, neither a respective key import nor key
 1414 generation can be expected here.

1415 FCS_CKM.4 Cryptographic key destruction not fulfilled,
 1416 but **justified**:
 1417 A hash function does not use any cryptographic key;
 1418 hence, a respective key destruction cannot be
 1419 expected here.

1420 FCS_COP.1.1/SHA_EAC2PP

1421 The TSF shall perform hashing⁹ in accordance with a specified cryptographic algorithm
 1422 SHA-1, SHA-224, SHA-256, SHA-384, SHA-512¹⁰ and cryptographic key sizes none¹¹ that
 1423 meet the following: [28]¹².

1424 **12. Application note (taken from [6], application note 13)**

1425 For compressing (hashing) an ephemeral public key for DH (TA2 and CA2), the hash function
 1426 SHA-1 shall be used ([18]). The TOE shall implement as hash functions either SHA-1 or SHA-
 1427 224 or SHA-256 for Terminal Authentication 2, cf. [18]. Within the normative Appendix of [18]
 1428 'Key Derivation Function', it is stated that the hash function SHA-1 shall be used for deriving
 1429 128-bit AES keys, whereas SHA-256 shall be used for deriving 192-bit and 256-bit AES keys.

1430 FCS_COP.1/SIG_VER_EAC2PP

1431 Cryptographic operation – Signature verification

1432 Hierarchical to: No other components

1433 Dependencies: [FDP_ITC.1 Import of user data without security
 1434 attributes, or FDP_ITC.2 Import of user data with
 1435 security attributes, or FCS_CKM.1 Cryptographic key
 1436 generation] not fulfilled, but **justified**:
 1437 The root key PK_{CVCA} (initialization data) used for
 1438 verifying the DV Certificate is stored in the TOE during
 1439 its personalization in the card issuing life cycle phase¹³.
 1440 Since importing the respective certificates (Terminal
 1441 Certificate, DV Certificate) does not require any special
 1442 security measures except those required by the current
 1443 SFR (cf. FMT_MTD.3/EAC2PP below), the current ST
 1444 does not contain any dedicated requirement like
 1445 FDP_ITC.2 for the import function.

1446 FCS_CKM.4 Cryptographic key destruction not fulfilled,
 1447 but **justified**:
 1448 Cryptographic keys used for the purpose of the current
 1449 SFR (PK_{PCD}, PK_{DV}, PK_{CVCA}) are public keys; they do
 1450 not represent any secret, and hence need not to be
 1451 destroyed.

⁹ [assignment: *list of cryptographic operations*]

¹⁰ [assignment: *cryptographic algorithm*]

¹¹ [assignment: *cryptographic key sizes*]

¹² [assignment: *list of standards*]

¹³ as already mentioned, operational use of the TOE is explicitly in focus of the ST and in the [20]

1452 FCS_COP.1.1/SIG_VER_EAC2PP

1453 The TSF shall perform digital signature verification¹⁴ in accordance with a specified
 1454 cryptographic algorithm RSA, RSA CRT and ECDSA¹⁵ and cryptographic key sizes RSA:
 1455 RSA, RSA CRT: 1024, 1280, 1536, 1984, 2048, 3072, 4096 and from 2000 bit to 4096 bit
 1456 in one bit steps; ECDSA: 160, 192, 224, 256, 320, 384, 521 bit¹⁶ that meet the following:
 1457 [24], [29]¹⁷.

1458 **13. Application note (taken from [6], application note 14)**

1459 This SFR is concerned with Terminal Authentication 2, cf. [17].

1460 **14. Application note (from ST author)**

1461 The TOE based on the Platform functionalities supports RSA and RSA-CRT digital signature
 1462 algorithms and cryptographic key sizes 512 bits up to 4096 bits with equal security measures.
 1463 However, to fend off attackers with high attack potential an adequate key length must be used.

1464 FCS_COP.1/PACE_ENC_EAC2PP

1465 Cryptographic operation – Encryption/Decryption AES

1466 Hierarchical to: No other components

1467 Dependencies: FDP_ITC.1 Import of user data without security
 1468 attributes, or FDP_ITC.2 Import of user data with
 1469 security attributes, or FCS_CKM.1 Cryptographic key
 1470 generation] fulfilled by
 1471 FCS_CKM.1/DH_PACE_EAC2PP

1472 FCS_CKM.4 Cryptographic key destruction fulfilled by
 1473 FCS_CKM.4/EAC2PP

1474 FCS_COP.1.1/PACE_ENC_EAC2PP

¹⁴ [assignment: *list of cryptographic operations*]

¹⁵ [assignment: *cryptographic algorithm*]

¹⁶ [assignment: *cryptographic key sizes*]

¹⁷ [assignment: *list of standards*]

1475 The TSF shall perform secure messaging – encryption and decryption¹⁸ in accordance
 1476 with a specified cryptographic algorithm AES in CBC mode¹⁹ and cryptographic key sizes
 1477 128, 192, 256 bit²⁰ that meet the following: **[18]**²¹

1478 **15. Application note (taken from [6], application note 15)**

1479 This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging
 1480 with encryption of transmitted data. The related session keys are agreed between the TOE
 1481 and the terminal as part of either the PACE protocol (PACE-K_{Enc}) or Chip Authentication 2 (CA-
 1482 K_{Enc}) according to FCS_CKM.1/DH_PACE_EAC2PP. Note that in accordance with [18], 3DES
 1483 could be used in CBC mode for secure messaging. Due to the fact that 3DES is not
 1484 recommended any more (cf. [17]), 3DES in any mode is no longer applicable here.

1485 **16. Application note (taken from [6], application note 16)**

1486 Refinement of FCS_COP.1.1/PACE_ENC_EAC2PP, since here PACE must adhere to [18].
 1487 All references (both the one in [13] and [18]) itself reference [12] for secure messaging. [18]
 1488 however further restricts the available choice of key-sizes and algorithms. Hence, [18] is fully
 1489 (backward) compatible to the reference given in [13].

1490 FCS_COP.1/PACE_MAC_EAC2PP
 1491 Cryptographic operation – MAC

1492 Hierarchical to: No other components

1493 Dependencies: FDP_ITC.1 Import of user data without security
 1494 attributes, or FDP_ITC.2 Import of user data with
 1495 security attributes, or FCS_CKM.1 Cryptographic key
 1496 generation] fulfilled by
 1497 FCS_CKM.1/DH_PACE_EAC2PP

1498 FCS_CKM.4 Cryptographic key destruction fulfilled by
 1499 FCS_CKM.4/EAC2PP

1500 FCS_COP.1.1/PACE_MAC_EAC2PP

¹⁸ [assignment: *list of cryptographic operations*]

¹⁹ [selection: *cryptographic algorithm*]

²⁰ [selection: *128, 192, 256 bit*]

²¹ [assignment: *list of standards*]

1501 The TSF shall perform secure messaging – message authentication code²² in accordance
 1502 with a specified cryptographic algorithm CMAC²³ and cryptographic key sizes 128, 192,
 1503 256 bit²⁴ that meet the following: **[18]**²⁵

1504 **17. Application note (redefined by ST author, taken from [6], application note 17)**

1505 See 16. Application note (taken from [6], application note 16).

1506 **18. Application note (taken from [6], application note 18)**

1507 This SFR removes 3DES and restricts to CMAC compared to the SFR of [13] by selection.
 1508 Hence, a minimum key-size of 128 bit is required.

1509 FCS_CKM.4/EAC2PP

1510 Cryptographic key destruction – Session keys

1511 Hierarchical to: No other components

1512 Dependencies: FDP_ITC.1 Import of user data without security
 1513 attributes, or FDP_ITC.2 Import of user data with
 1514 security attributes, or FCS_CKM.1 Cryptographic key
 1515 generation] fulfilled by
 1516 FCS_CKM.1/DH_PACE_EAC2PP and
 1517 FCS_CKM.1/CA_EAC1PP

1518 FCS_CKM.4.1/EAC2PP

1519 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic
 1520 key destruction method physically overwriting the keys in a randomized manner²⁶ that
 1521 meets the following: provided by the underlying certified Platform²⁷.

1522 **19. Application note**

1523 In [13] concerning this component requires the destruction of PACE session keys after
 1524 detection of an error in a received command by verification of the MAC. While the definition of
 1525 FCS_CKM.4/EAC2PP remains unaltered, here this component also requires the destruction
 1526 of sessions keys after a successful run of Chip Authentication 2. The TOE shall destroy the
 1527 CA2 session keys after detection of an error in a received command by verification of the MAC.
 1528 The TOE shall clear the memory area of any session keys before starting the communication
 1529 with the terminal in a new after-reset-session as required by FDP_RIP.1/EAC2PP.

²² [assignment: *list of cryptographic operations*]

²³ [selection: *cryptographic algorithm*]

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

²⁵ [assignment: *list of standards*]

²⁶ [assignment: *cryptographic key destruction method*]

²⁷ [assignment: *list of standards*]

1530 FCS_RND.1/EAC2PP

1531 Quality metric for random numbers

1532 Hierarchical to: No other components

1533 Dependencies: No dependencies.

1534 FCS_RND.1.1/EAC2PP

1535 The TSF shall provide a mechanism to generate random numbers that meet DRG.3²⁸.

1536 **20. Application note**

1537 In [13] concerning this component requires the TOE to generate random numbers (random
1538 nonce) for PACE. While the definition of FCS_RND.1/EAC2PP remains unaltered, here this
1539 component requires the TOE to generate random numbers (random nonce) for all
1540 authentication protocols (i.e. PACE, CA2), as required by FIA_UAU.4/PACE_EAC2PP.

1541 The following SFRs are imported due to claiming [5]. They concern cryptographic support for
1542 applications that contain EAC1-protected data groups.

1543 • **FCS_CKM.1/DH_PACE_EAC1PP**

1544 • **FCS_CKM.4/EAC1PP**

1545 (equivalent to **FCS_CKM.4/EAC2PP**, but listed here for the sake of completeness)

1546 • **FCS_COP.1/PACE_ENC_EAC1PP**

1547 • **FCS_COP.1/PACE_MAC_EAC1PP**

1548 **21. Application note (redefined by ST author, taken from[20], application note 9)**

1549 Applied.

1550 • **FCS_RND.1/EAC1PP**

1551 (equivalent to **FCS_RND.1/EAC2PP**, but listed here for the sake of completeness)

1552 • **FCS_CKM.1/CA_EAC1PP**

1553 • **FCS_COP.1/CA_ENC_EAC1PP**

1554 • **FCS_COP.1/SIG_VER_EAC1PP**

1555 • **FCS_COP.1/CA_MAC_EAC1PP**

²⁸ [assignment: a defined quality metric]

- 1556 FCS_CKM.1/DH_PACE_EAC1PP
 1557 Cryptographic key generation – Diffie-Hellman for PACE session keys
- 1558 Hierarchical to: No other components
- 1559 Dependencies: [FCS_CKM.2 Cryptographic key distribution or
 1560 FCS_COP.1 Cryptographic operation].
 1561 **Justification:** A Diffie-Hellman key agreement is used
 1562 in order to have no key distribution, therefore
 1563 FCS_CKM.2 makes no sense in this case.
- 1564 FCS_CKM.4 Cryptographic key destruction: fulfilled by
 1565 FCS_CKM.4/EAC1PP
- 1566 FCS_CKM.1.1/DH_PACE_EAC1PP
- 1567 The TSF shall generate cryptographic keys in accordance with a specified cryptographic
 1568 key generation algorithm Diffie-Hellman-Protocol compliant to [27], ECDH compliant to
 1569 [26]²⁹³⁰ and specified cryptographic key sizes TDES 128, AES 128, 192 and 256 bits³¹ that
 1570 meet the following:[7]³²
- 1571 FCS_COP.1/PACE_ENC_EAC1PP
 1572 Encryption / Decryption AES / 3DES
- 1573 Hierarchical to: No other components
- 1574 Dependencies: [FDP_ITC.1 Import of user data without security
 1575 attributes, or FDP_ITC.2 Import of user data with
 1576 security attributes, or FCS_CKM.1 Cryptographic key
 1577 generation]: fulfilled by
 1578 FCS_CKM.1/DH_PACE_EAC1PP.
- 1579 FCS_CKM.4 Cryptographic key destruction: fulfilled by
 1580 FCS_CKM.4/EAC1PP.
- 1581 FCS_COP.1.1/PACE_ENC_EAC1PP

²⁹ [assignment: *cryptographic key generation algorithm*]

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

³¹ [assignment: *cryptographic key sizes*]

³² [assignment: *list of standards*]

1582 The TSF shall perform secure messaging – encryption and decryption³³ in accordance
 1583 with a specified cryptographic algorithm AES, 3DES³⁴ in CBC mode³⁵ and cryptographic
 1584 key sizes 3DES 112, AES 128, 192, 256 bit³⁶³⁷ that meet the following: compliant to [7]³⁸.

1585 FCS_COP.1/PACE_MAC_EAC1PP
 1586 Cryptographic operation – MAC

1587 Hierarchical to: No other components

1588 Dependencies: [FDP_ITC.1 Import of user data without security
 1589 attributes, or FDP_ITC.2 Import of user data with
 1590 security attributes, or FCS_CKM.1 Cryptographic key
 1591 generation]: fulfilled by
 1592 FCS_CKM.1/DH_PACE_EAC1PP
 1593 FCS_CKM.4 Cryptographic key destruction: fulfilled by
 1594 FCS_CKM.4/EAC1PP.

1595 FCS_COP.1.1/PACE_MAC_EAC1PP

1596 The TSF shall perform secure messaging – message authentication code³⁹ in accordance
 1597 with a specified cryptographic algorithm CMAC, Retail-MAC⁴⁰⁴¹ and cryptographic key
 1598 sizes 3DES 112, AES 128, 192, 256 bit⁴²⁴³ that meet the following: compliant to [7]⁴⁴.

1599 FCS_CKM.1/CA_EAC1PP
 1600 Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys

1601 Hierarchical to: No other components

1602 Dependencies: [FCS_CKM.2 Cryptographic key distribution or
 1603 FCS_COP.1 Cryptographic operation] fulfilled by

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

- 1604 FCS_COP.1/CA_ENC_EAC1PP and
1605 FCS_COP.1/CA_MAC_EAC1PP
- 1606 FCS_CKM.4 Cryptographic key destruction fulfilled by
1607 FCS_CKM.4/EAC1PP.
- 1608 FCS_CKM.1.1/CA_EAC1PP
- 1609 The TSF shall generate cryptographic keys in accordance with a specified cryptographic
1610 key generation algorithm Diffie-Hellman protocol compliant to PKCS#3 and based on an
1611 ECDH protocol⁴⁵ and specified cryptographic key sizes TDES 112, AES 128, 192 and 256
1612 bits⁴⁶ that meet the following: based on the Diffie-Hellman key derivation protocol compliant
1613 to [27] and [16] , based on an ECDH protocol compliant to [26]^{47,48}
- 1614 **22. Application note (taken from [5], application note 12)**
- 1615 FCS_CKM.1/CA_EAC1PP implicitly contains the requirements for the hashing functions used
1616 for key derivation by demanding compliance to [16].
- 1617 **23. Application note (taken from [5], application note 13)**
- 1618 The TOE generates a shared secret value with the terminal during the Chip Authentication
1619 Protocol Version 1, see [16]. This protocol may be based on the Diffie-Hellman-Protocol
1620 compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [27]) or on the
1621 ECDH compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm) (cf. [26], for
1622 details). The shared secret value is used to derive the Chip Authentication Session Keys used
1623 for encryption and MAC computation for secure messaging (defined in Key Derivation Function
1624 [16]).
- 1625 **24. Application note (taken from [5], application note 14)**
- 1626 The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the
1627 keys for secure messaging from any shared secrets of the Authentication Mechanisms. The
1628 Chip Authentication Protocol v.1 may use SHA-1 (cf. [16]). The TOE may implement additional
1629 hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol v.1 (cf. [16] for
1630 details).
- 1631 **25. Application note (taken from [5], application note 15)**
- 1632 The TOE shall destroy any session keys in accordance with FCS_CKM.4 from [13] after (i)
1633 detection of an error in a received command by verification of the MAC and (ii) after successful
1634 run of the Chip Authentication Protocol v.1. (iii) The TOE shall destroy the PACE Session Keys
1635 after generation of a Chip Authentication Session Keys and changing the secure messaging
1636 to the Chip Authentication Session Keys. (iv) The TOE shall clear the memory area of any

⁴⁵ [assignment: *cryptographic key generation algorithm*]

⁴⁶ [assignment: *cryptographic key sizes*]

⁴⁷ [assignment: *list of standards*]

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

1637 session keys before starting the communication with the terminal in a new after-reset-session
 1638 as required by FDP_RIP.1/EAC1PP. Concerning the Chip Authentication keys
 1639 FCS_CKM.4/EAC1PP is also fulfilled by FCS_CKM.1/CA_EAC1PP.

1640 FCS_COP.1/CA_ENC_EAC1PP

1641 Cryptographic operation – Symmetric Encryption / Decryption

1642 Hierarchical to: No other components

1643 Dependencies: [FDP_ITC.1 Import of user data without security
 1644 attributes, or FDP_ITC.2 Import of user data with
 1645 security attributes, or FCS_CKM.1 Cryptographic key
 1646 generation] fulfilled by FCS_CKM.1/CA_EAC1PP

1647 FCS_CKM.4 Cryptographic key destruction fulfilled by
 1648 FCS_CKM.4/EAC1PP

1649 FCS_COP.1.1/CA_ENC_EAC1PP

1650 The TSF shall perform secure messaging – encryption and decryption⁴⁹ in accordance
 1651 with a specified cryptographic algorithm Triple-DES and AES⁵⁰ and cryptographic key
 1652 sizes Triple-DES:112, AES: 128, 192 and 256 bits⁵¹ that meet the following:[16]⁵².

1653 **26. Application note (taken from [5], application note 16)**

1654 This SFR requires the TOE to implement the cryptographic primitives (e.g. Triple-DES and/or
 1655 AES) for secure messaging with encryption of the transmitted data. The keys are agreed
 1656 between the TOE and the terminal as part of the Chip Authentication Protocol Version 1
 1657 according to the FCS_CKM.1/CA_EAC1PP.

1658 FCS_COP.1/SIG_VER_EAC1PP

1659 Cryptographic operation – Signature verification by electronic document

1660 Hierarchical to: No other components

1661 Dependencies: [FDP_ITC.1 Import of user data without security
 1662 attributes, or FDP_ITC.2 Import of user data with
 1663 security attributes, or FCS_CKM.1 Cryptographic key
 1664 generation] fulfilled by FCS_CKM.1/CA_EAC1PP

⁴⁹ [assignment: *list of cryptographic operations*]

⁵⁰ [assignment: *cryptographic algorithm*]

⁵¹ [assignment: *cryptographic key sizes*]

⁵² [assignment: *list of standards*]

- 1665 FCS_CKM.4 Cryptographic key destruction fulfilled by
- 1666 FCS_CKM.4/EAC1PP

- 1667 FCS_COP.1.1/SIG_VER_EAC1PP

- 1668 The TSF shall perform digital signature verification⁵³ in accordance with a specified
- 1669 cryptographic algorithm RSA v1.5 with SHA-256 and SHA-512, RSA-PSS with SHA-256
- 1670 and SHA-512, ECDSA with SHA-256, SHA-224, SHA-384 and SHA-512⁵⁴ and
- 1671 cryptographic key sizes RSA 2048, 4096 and from 2000 bit to 4096 bit in one bit steps,
- 1672 ECDSA 160, 192, 224, 256, 320, 384, 521 bits⁵⁵ that meet the following: [24][29]⁵⁶.

- 1673 **27. Application note (redefined by ST author, taken from [5], application note 17)**

- 1674 Applied.

- 1675 **28. Application note (from ST author)**

- 1676 The TOE based on the Platform functionalities supports RSA and RSA-CRT digital signature
- 1677 algorithms and cryptographic key sizes 512 bits up to 4096 bits with equal security measures.
- 1678 However, to fend off attackers with high attack potential an adequate key length must be used.

- 1679 FCS_COP.1/CA_MAC_EAC1PP
- 1680 Cryptographic operation – MAC

- 1681 Hierarchical to: No other components

- 1682 Dependencies: [FDP_ITC.1 Import of user data without security
- 1683 attributes, or FDP_ITC.2 Import of user data with
- 1684 security attributes, or FCS_CKM.1 Cryptographic key
- 1685 generation] fulfilled by FCS_CKM.1/CA_EAC1PP

- 1686 FCS_CKM.4 Cryptographic key destruction fulfilled by
- 1687 FCS_CKM.4/EAC1PP

- 1688 FCS_COP.1.1/CA_MAC_EAC1PP

⁵³ [assignment: *list of cryptographic operations*]

⁵⁴ [assignment: *cryptographic algorithm*]

⁵⁵ [assignment: *cryptographic key sizes*]

⁵⁶ [assignment: *list of standards*]

1689 The TSF shall perform secure messaging – message authentication code⁵⁷ in accordance
 1690 with a specified cryptographic algorithm CMAC or Retail-MAC⁵⁸ and cryptographic key
 1691 sizes 112, 128, 192 and 256 bits⁵⁹ that meet the following: [16]⁶⁰.

1692 **29. Application note (taken from [5], application note 18)**

1693 This SFR requires the TOE to implement the cryptographic primitive for secure messaging with
 1694 encryption and message authentication code over the transmitted data. The key is agreed
 1695 between the TSF by Chip Authentication Protocol Version 1 according to the
 1696 FCS_CKM.1/CA_EAC1PP. Furthermore, the SFR is used for authentication attempts of a
 1697 terminal as Personalisation Agent by means of the authentication mechanism.

1698 The following SFRs are defined because the TOE supports the Chip Authentication version 2
 1699 and Restricted Identification key pair(s) generation on the TOE as described in
 1700 FMT_MTD.1/SK_PICC_EAC2PP.

1701 **FCS_CKM.1/CA2**

1702 **Cryptographic key generation – Chip Authentication version 2 Key pair(s)**

1703 Hierarchical to: No other components

1704 Dependencies: [FCS_CKM.2 Cryptographic key distribution or
 1705 FCS_COP.1 Cryptographic operation]
 1706 fulfilled by FCS_COP.1/PACE_ENC_EAC2PP and
 1707 FCS_COP.1/PACE_MAC_EAC2PP

1708 FCS_CKM.4 Cryptographic key destruction fulfilled by
 1709 FCS_CKM.4/EAC2PP

1710 **FCS_CKM.1.1/CA2**

1711 The TSF shall generate cryptographic keys to **Chip Authentication 2** in accordance with a
 1712 specified cryptographic key generation algorithm RSA or ECC⁶¹ and specified cryptographic
 1713 key sizes 1024, 1280, 1536, 1984, 2048, 3072 and 4096 bits or 160, 192, 224, 256, 384 and
 1714 521 bits⁶² that meet the following: [31]⁶³.

1715 **30. Application note (from ST author)**

1716 The TOE supports to create Chip Authentication version 2 Key pair(s) on the TOE as described
 1717 in FMT_MTD.1/SK_PICC_EAC2PP. The TOE generates the key pair(s) in secure way, but the

⁵⁷ [assignment: *list of cryptographic operations*]

⁵⁸ [assignment: *cryptographic algorithm*]

⁵⁹ [assignment: *cryptographic key sizes*]

⁶⁰ [assignment: *list of standards*]

⁶¹ [assignment: *cryptographic key generation algorithm*]

⁶² [assignment: *cryptographic key sizes*]

⁶³ [assignment: *list of standards*]

1718 appropriate key size shall be assessed during the personalization of the TOE.
 1719 The refinement was necessary for the sake of clarity.

1720 FCS_CKM.1/RI
 1721 Cryptographic key generation – Restricted Identification Key pair (s)

1722 Hierarchical to: No other components

1723 Dependencies: [FCS_CKM.2 Cryptographic key distribution or
 1724 FCS_COP.1 Cryptographic operation] not fulfilled but
 1725 justified: the cryptographic part of Restricted
 1726 Identification protocol is not part of the TOE, so no
 1727 cryptographic operation is related to FCS_CKM.1/RI.
 1728 FCS_CKM.4 Cryptographic key destruction fulfilled by
 1729 FCS_CKM.4/EAC2PP

1730 FCS_CKM.1.1/RI

1731 The TSF shall generate cryptographic keys **to Restricted Identification** in accordance with a
 1732 specified cryptographic key generation algorithm RSA or ECC⁶⁴ and specified cryptographic
 1733 key sizes 1024, 1280, 1536, 1984, 2048, 3072 and 4096 bits or 160, 192, 224, 256, 384 and
 1734 521 bits⁶⁵ that meet the following: [31][17]⁶⁶.

1735 **31. Application note (from ST author)**

1736 The TOE supports to create Restricted Identification Key pair(s) on the TOE as described in
 1737 FMT_MTD.1/SK_PICC_EAC2PP. The TOE generates the key pair(s) in secure way, but the
 1738 appropriate key size shall be assessed during the personalization of the TOE.
 1739 The refinement was necessary for the sake of clarity.

1740 The following SFRs are new and concern cryptographic support for ePassport application in
 1741 combination with [5] in case the Active Authentication protocol is active:

- 1742 • **FCS_CKM.1/AA**
- 1743 • **FCS_COP.1/AA**

1744 FCS_CKM.1/AA
 1745 Cryptographic key generation – Active Authentication Key Pair

1746 Hierarchical to: No other components

⁶⁴ [assignment: *cryptographic key generation algorithm*]

⁶⁵ [assignment: *cryptographic key sizes*]

⁶⁶ [assignment: *list of standards*]

- 1747 Dependencies: [FCS_CKM.2 Cryptographic key distribution or
- 1748 FCS_COP.1 Cryptographic operation]
- 1749 fulfilled by FCS_COP.1/AA

- 1750 FCS_CKM.4 Cryptographic key destruction fulfilled by
- 1751 FCS_CKM.4/EAC1PP

- 1752 FCS_CKM.1.1/AA

- 1753 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key
- 1754 generation algorithm RSA or ECDSA⁶⁷ and specified cryptographic key sizes 1024, 1280,
- 1755 1536, 1984, 2048, 3072 and 4096 bits or 160, 192, 224, 256, 384 and 521 bits⁶⁸ that meet the
- 1756 following: [7][9]⁶⁹.

- 1757 FCS_COP.1/AA
- 1758 Cryptographic operation – Active Authentication

- 1759 Hierarchical to: No other components

- 1760 Dependencies: [FDP_ITC.1 Import of user data without security
- 1761 attributes, FDP_ITC.2 Import of user data with security
- 1762 attribute or FCS_CKM.1 Cryptographic key generation]
- 1763 fulfilled by FCS_CKM.1/AA

- 1764 FCS_CKM.4 Cryptographic key destruction fulfilled by
- 1765 FCS_CKM.4/EAC1PP

- 1766 FCS_COP.1.1/AA

- 1767 The TSF shall perform digital signature creation⁷⁰ in accordance with a specified
- 1768 cryptographic algorithm RSA or ECDSA⁷¹ and . cryptographic key sizes RSA with key
- 1769 sizes 2048-4096 and ECDSA with key sizes 160-521⁷² that meet the following: [7][9]⁷³.

- 1770 The following SFRs are new and concerns cryptographic support for ePassport applications in
- 1771 combination with [5].

- 1772
 - **FCS_CKM.1/CAM**

⁶⁷ [assignment: *cryptographic key generation algorithm*]

⁶⁸ [assignment: *cryptographic key sizes*]

⁶⁹ [assignment: *list of standards*]

⁷⁰ [assignment: *list of cryptographic operations*]

⁷¹ [assignment: *cryptographic algorithm*]

⁷² [assignment: *cryptographic key sizes*]

⁷³ [assignment: *list of standards*]

1773 • **FCS_COP.1/CAM**

1774 FCS_CKM.1/CAM

1775 Cryptographic key generation – PACE-CAM public key and Diffie-Hellman for General Mapping in
1776 PACE-GM

1777 Hierarchical to: No other components

1778 Dependencies: [FCS_CKM.2 Cryptographic key distribution or
1779 FCS_COP.1 Cryptographic operation]
1780 fulfilled by FCS_COP.1/CAM

1781 FCS_CKM.4 Cryptographic key destruction
1782 fulfilled by FCS_CKM.4/EAC1PP

1783 FCS_CKM.1.1/CAM

1784 The TSF shall generate cryptographic keys in accordance with a specified cryptographic
1785 key generation algorithm PACE-CAM in combination with PACE-GM⁷⁴ and specified
1786 cryptographic key sizes AES 128, 192 and 256 bit⁷⁵ that meet the following: [9]⁷⁶.

1787 **32. Application note (from ST author)**

1788 In the combined protocol PACE-CAM, after the completion of PACE in combination with the
1789 general mapping (PACE-GM), the chip authenticates itself by adding (multiplying) the
1790 randomly chosen nonce of the GM step with the inverse of the chip authentication secret key,
1791 and sends this value together with chip authentication public key to the card; cf.[9].

1792 FCS_COP.1/CAM

1793 Cryptographic operation – PACE-CAM

1794 Hierarchical to: No other components

1795 Dependencies: [FDP_ITC.1 Import of user data without security
1796 attributes, or FDP_ITC.2 Import of user data with
1797 security attributes, or FCS_CKM.1 Cryptographic key
1798 generation]
1799 fulfilled by FCS_CKM.1/CAM

⁷⁴ [assignment: *cryptographic key generation algorithm*]

⁷⁵ [assignment: *cryptographic key sizes*]

⁷⁶ [assignment: *list of standards*]

1800		FCS_CKM.4 Cryptographic key destruction
1801		fulfilled by FCS_CKM.4/EAC1PP
1802	FCS_COP.1.1/CAM	
1803	The TSF shall perform <u>the PACE-CAM protocol</u> ⁷⁷ in accordance with a specified	
1804	cryptographic algorithm <u>PACE-CAM</u> ⁷⁸ and cryptographic key sizes <u>AES 128, 192 and 256</u>	
1805	<u>bits</u> ⁷⁹ that meet the following: <u>[9]</u> ⁸⁰	
1806	33. Application note (from ST author)	
1807	Whereas FCS_CKM.1/CAM addresses the Diffie-Hellman based key-derivation, this SFR is	
1808	concerned with the correct implementation and execution of the whole PACE-CAM protocol.	
1809	Note that in particular the last protocol step to authenticate the chip towards the terminal is an	
1810	essential part of the protocol, and not addressed in FCS_CKM.1/CAM.	
1811	The following SFRs are imported due to claiming [14]. They only concern the cryptographic	
1812	support for an eSign application.	
1813	<ul style="list-style-type: none"> • FCS_CKM.1/SSCDPP 	
1814	<ul style="list-style-type: none"> • FCS_CKM.4/SSCDPP 	
1815	(equivalent to FCS_CKM.4/EAC2PP, but listed here for the sake of completeness)	
1816	<ul style="list-style-type: none"> • FCS_COP.1/SSCDPP 	
1817	FCS_CKM.1/SSCDPP	
1818	Cryptographic key generation	
1819	Hierarchical to:	No other components
1820	Dependencies:	FCS_CKM.2 Cryptographic key distribution, or
1821		FCS_COP.1 Cryptographic operation] fulfilled by
1822		FCS_COP.1/SSCDPP
1823		FCS_CKM.4 Cryptographic key destruction fulfilled by
1824		FCS_CKM.4/EAC2PP
1825	FCS_CKM.1.1/SSCDPP	

⁷⁷ [assignment: *list of cryptographic operations*]

⁷⁸ [assignment: *cryptographic algorithm*]

⁷⁹ [assignment: *cryptographic key sizes*]

⁸⁰ [assignment: *list of standards*]

1826 The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic
 1827 key generation algorithm RSA or ECDSA⁸¹ and specified cryptographic key sizes 1024,
 1828 1280, 1536, 1984, 2048, 3072 and 4096 bits or 160, 192, 224, 256, 384 and 521 bits⁸²
 1829 that meet the following: [23]⁸³.

1830 **34. Application note (taken from [14], application note 5)**

1831 The ST writer performed the missing operations in the element FCS_CKM.1.1/SSCDPP. The
 1832 refinement in the element FCS_CKM.1.1 SSCDPP substitutes “cryptographic keys” by
 1833 “SCD/SVD pairs” because it clearly addresses the SCD/SVD key generation.

1834 FCS_COP.1/SSCDPP
 1835 Cryptographic operation

1836 Hierarchical to: No other components

1837 Dependencies: FDP_ITC.1 Import of user data without security
 1838 attributes, FDP_ITC.2 Import of user data with security
 1839 attribute or FCS_CKM.1 Cryptographic key generation]
 1840 fulfilled by FCS_CKM.1/SSCDPP
 1841 FCS_CKM.4 Cryptographic key destruction fulfilled by
 1842 FCS_CKM.4/EAC2PP

1843 FCS_COP.1.1/SSCDPP

1844 The TSF shall perform digital signature creation⁸⁴ in accordance with a specified
 1845 cryptographic algorithm RSA according to RSASSA-PKCS1-v1_5, RSASSA-PSS or
 1846 ECDSA according to ISO14883-3⁸⁵ and . cryptographic key sizes RSA with key sizes
 1847 2048-4096 and ECDSA with key sizes 160-521⁸⁶ that meet the following: [24] [29]⁸⁷.

1848 **35. Application note (taken from [14], application note 7)**

1849 Applied.

1850 **36. Application note (from ST author)**

1851 The underlying Platform supports RSA, RSA-CRT and ECDSA digital signature algorithms and
 1852 cryptographic key sizes 2048 bits to 4096 bits (RSA) and 160 bits to 521 bits (ECDSA) with

⁸¹ [assignment: *cryptographic key generation algorithm*]

⁸² [assignment: *cryptographic key sizes*]

⁸³ [assignment: *list of standards*]

⁸⁴ [assignment: *list of cryptographic operations*]

⁸⁵ [assignment: *cryptographic algorithm*]

⁸⁶ [assignment: *cryptographic key sizes*]

⁸⁷ [assignment: *list of standards*]

1853 equal security measures. However, to fend off attackers with high attack potential an adequate
 1854 key length must be used

1855 **6.1.2. Class FIA**

1856 Table 10 provides an overview of the authentication and identification mechanisms used.

Name	SFR for the TOE
PACE protocol	FIA_UID.1/PACE_EAC2PP
	FIA_UAU.5/PACE_EAC2PP
	FIA_AFL.1/Suspend_PIN_EAC2PP
	FIA_AFL.1/Block_PIN_EAC2PP
	FIA_AFL.1/PACE_EAC2PP
	FIA_AFL.1/PACE_EAC1PP
PACE-CAM protocol	SFRs above for the PACE part; in addition, for the Chip Authentication Mapping (CAM): FIA_API.1/PACE_CAM FIA_UAU.5/PACE_EAC1PP
Terminal Authentication Protocol version 2	FIA_UAU.1/EAC2_Terminal_EAC2PP
	FIA_UAU.5/PACE_EAC2PP
Chip Authentication Protocol version 2	FIA_API.1/CA_EAC2PP
	FIA_UAU.5/PACE_EAC2PP
	FIA_UAU.6/PACE_EAC2PP
Terminal Authentication Protocol version 1	FIA_UAU.1/PACE_EAC1PP
	FIA_UAU.5/PACE_EAC1PP
Chip Authentication Protocol version 1	FIA_API.1/EAC1PP
	FIA_UAU.5/PACE_EAC1PP
	FIA_UAU.6/EAC_EAC1PP
Active Authentication	FIA_API.1/AA
	FIA_UAU.1/PACE_EAC1PP
	FIA_UAU.4/PACE_EAC1PP
Restricted Identification	FIA_API.1/RI_EAC2PP
eSign-PIN	FIA_UAU.1/SSCDPP

1857 *Table 10 Overview of authentication and identification SFRs*

1858 **6.1.2.1. SFRs for EAC2-protected Data**

1859 The following SFRs are imported due to claiming [6]. They mainly concern authentication
 1860 mechanisms related to applications with EAC2-protected data.

- 1861 • **FIA_AFL.1/Suspend_PIN_EAC2PP**
- 1862 • **FIA_AFL.1/Block_PIN_EAC2PP**
- 1863 • **FIA_API.1/CA_EAC2PP**
- 1864 • **FIA_API.1/RI_EAC2PP**
- 1865 • **FIA_UID.1/PACE_EAC2PP**
- 1866 • **FIA_UID.1/EAC2_Terminal_EAC2PP**

1867 **37. Application note (taken from [20], application note 10)**

1868 The user identified after a successfully performed TA2 protocol is an EAC2 terminal. Note that
 1869 TA1 is covered by FIA_UID.1/PACE_EAC1PP. In that case, the terminal identified is in addition
 1870 also an EAC1 terminal.

- 1871 • **FIA_UAU.1/PACE_EAC2PP**
- 1872 • **FIA_UAU.1/EAC2_Terminal_EAC2PP**
- 1873 • **FIA_UAU.4/PACE_EAC2PP**

1874 **38. Application note (taken from [6], application note 26)**

1875 For PACE, the TOE randomly selects an almost uniformly distributed nonce of 128 bit length.
 1876 The [20] and the current ST support a key derivation function based on AES; see [17]. For
 1877 TA2, the TOE randomly selects a nonce r_{PICC} of 64 bit length, see [17]. This SFR extends
 1878 FIA_UAU.4/PACE_EAC1PP from [13] by assigning the authentication mechanism Terminal
 1879 Authentication 2.

- 1880 • **FIA_UAU.5/PACE_EAC2PP**
- 1881 • **FIA_UAU.6/CA_EAC2PP**
- 1882 • **FIA_AFL.1/PACE_EAC2PP**
- 1883 • **FIA_UAU.6/PACE_EAC2PP**

1884 FIA_AFL.1/Suspend_PIN_EAC2PP
 1885 Authentication failure handling – Suspending PIN

1886 Hierarchical to: No other components

1887 Dependencies: [FIA_UAU.1 Timing of authentication] fulfilled by
 1888 FIA_UAU.1/PACE_EAC2PP

1889 FIA_AFL.1.1/Suspend_PIN_EAC2PP

1890 The TSF shall detect when an administrator configurable positive integer within [1-127]⁸⁸
 1891 unsuccessful authentication attempts occur related to consecutive failed authentication
 1892 attempts using the PIN as the shared password for PACE⁸⁹.

1893 FIA_AFL.1.2/Suspend_PIN_EAC2PP

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

⁸⁹ [assignment: list of authentication events]

1894 When the defined number of unsuccessful authentication attempts has been met⁹⁰, the
 1895 TSF shall suspend the reference value of the PIN according to [17]⁹¹.

1896 **39. Application note (taken from [6], application note 19)**

1897 This SFR is not in conflict to FIA_AFL.1 from [13], since it just adds a requirement specific to
 1898 the case where the PIN is the shared password. Thus, the assigned integer number for
 1899 unsuccessful authentication attempts with any PACE password could be different to the integer
 1900 for the case when using a PIN.

1901 FIA_AFL.1/Block_PIN_EAC2PP
 1902 Authentication failure handling – Blocking PIN

1903 Hierarchical to: No other components

1904 Dependencies: [FIA_UAU.1 Timing of authentication] fulfilled by
 1905 FIA_UAU.1/PACE_EAC2PP

1906 FIA_AFL.1.1/Block_PIN_EAC2PP

1907 The TSF shall detect when an administrator configurable positive integer within [1-127]⁹²
 1908 unsuccessful authentication attempts occur related to consecutive failed authentication
 1909 attempts using the suspended⁹³ PIN as the shared password for PACE⁹⁴.

1910 FIA_AFL.1.2/Block_PIN_EAC2PP

1911 When the defined number of unsuccessful authentication attempts has been met⁹⁵, the
 1912 TSF shall block the reference value of PIN according to [17]⁹⁶.

1913 FIA_API.1/CA_EAC2PP
 1914 Authentication Proof of Identity

1915 Hierarchical to: No other components

1916 Dependencies: No dependencies

1917 FIA_API.1.1/CA_EAC2PP

⁹⁰ [selection: *met*, *surpassed*]

⁹¹ [assignment: *list of actions*]

⁹² [selection: [assignment: *positive integer number*], *an administrator configurable positive integer within [assignment: *range of acceptable values*]]*

⁹³ as required by FIA_AFL.1/Suspend_PIN_EAC2PP

⁹⁴ [assignment: *list of authentication events*]

⁹⁵ [selection: *met*, *surpassed*]

⁹⁶ [assignment: *list of actions*]

1918 The TSF shall provide the protocol Chip Authentication 2 according to [17]⁹⁷, to prove the
 1919 identity of the TOE⁹⁸.

1920 FIA_API.1/RI_EAC2PP
 1921 Authentication Proof of Identity

1922 Hierarchical to: No other components

1923 Dependencies: No dependencies

1924 FIA_API.1.1/RI_EAC2PP

1925 The TSF shall provide the Restricted Identification protocol according to [17]⁹⁹, to prove
 1926 the identity of the TOE¹⁰⁰.

1927 **40. Application note (taken from [6], application note 20)**

1928 Restricted Identification provides a sector-specific identifier of every electronic document. It
 1929 thus provides a pseudonymous way to identify the Electronic Document Holder in a case where
 1930 the CHAT of the terminal does not allow to access Sensitive User Data that directly identify the
 1931 Electronic Document Holder. Restricted Identification shall only be used after successfully
 1932 running Terminal Authentication 2 and Chip Authentication 2. Note that Restricted Identification
 1933 is optional according to [17], and thus the above SFR only applies if Restricted Identification is
 1934 supported by the TOE.

1935 FIA_UID.1/PACE_EAC2PP
 1936 Timing of identification

1937 Hierarchical to: No other components

1938 Dependencies: No dependencies

1939 FIA_UID.1.1/PACE_EAC2PP

1940 The TSF shall allow:

- 1941 1. to establish a communication channel,
- 1942 2. carrying out the PACE protocol according to [17]
- 1943 3. to read the Initialization Data if it is not disabled by TSF according to
 1944 ~~FMT_MTD.1/INI_DIS~~FMT_MTD.1/INI_DIS_EAC2PP¹⁰¹

⁹⁷ [assignment: *authentication mechanism*]

⁹⁸ [assignment: *authorised user or role, or of the TOE itself*]

⁹⁹ [assignment: *authentication mechanism*]

¹⁰⁰ [assignment: *authorized user or role*]

¹⁰¹ [assignment: *list of TSF-mediated actions*]

1945 4. none¹⁰²

1946 on behalf of the user to be performed before the user is identified.

1947 FIA_UID.1.2/PACE_EAC2PP

1948 The TSF shall require each user to be successfully identified before allowing any other

1949 TSF-mediated actions on behalf of that user.

1950 **41. Application note (taken from [6], application note 21)**

1951 The user identified after a successful run of PACE is a PACE terminal. In case the PIN or PUK

1952 were used for PACE, the user identified is the Electronic Document Holder using a PACE

1953 terminal. Note that neither the CAN nor the MRZ effectively represent secrets, but are

1954 restricted-revealable; i.e. in case the CAN or the MRZ were used for PACE, it is either the

1955 Electronic Document Holder itself, an authorized person other than the Electronic Document

1956 Holder, or a device.

1957 **42. Application note (from ST author)**

1958 The refinement was necessary to ensure unified terminology usage of SFRs.

1959 FIA_UID.1/EAC2_Terminal_EAC2PP

1960 Timing of identification

1961 Hierarchical to: No other components

1962 Dependencies: No dependencies

1963 FIA_UID.1.1/EAC2_Terminal_EAC2PP

1964 The TSF shall allow

- 1965 1. to establish a communication channel,
- 1966 2. carrying out the PACE protocol according to [17],
- 1967 3. to read the Initialization Data if it is not disabled by TSF according to
- 1968 **FMT_MTD.1/INI_DISFMT_MTD.1/INI_DIS_EAC2PP**
- 1969 4. carrying out the Terminal Authentication protocol 2 according to [17]¹⁰³
- 1970 5. none¹⁰⁴

1971 on behalf of the user to be performed before the user is identified.

1972 FIA_UID.1.2/EAC2_Terminal_EAC2PP

¹⁰² [assignment: list of TSF-mediated actions]

¹⁰³ [assignment: list of TSF-mediated actions]

¹⁰⁴ [assignment: list of TSF-mediated actions]

1973 The TSF shall require each user to be successfully identified before allowing any other
 1974 TSF-mediated actions on behalf of that user.

1975 **43. Application note (taken from [6], application note 22)**

1976 The user identified after a successfully performed TA2 is an EAC2 terminal. The types of EAC2
 1977 terminals are application dependent;

1978 **44. Application note (taken from [6], application note 23)**

1979 In the life cycle phase manufacturing, the manufacturer is the only user role known to the TOE.
 1980 The manufacturer writes the initialization data and/or pre-personalization data in the audit
 1981 records of the IC.

1982 Note that a Personalization Agent acts on behalf of the electronic document issuer under his
 1983 and the CSCA's and DS's policies. Hence, they define authentication procedures for
 1984 Personalization Agents. The TOE must functionally support these authentication procedures.
 1985 These procedures are subject to evaluation within the assurance components ALC_DEL.1 and
 1986 AGD_PRE.1. The TOE assumes the user role Personalization Agent, if a terminal proves the
 1987 respective Terminal Authorization level (e. g. a privileged terminal, cf. [17]).

1988 **45. Application note (from ST author)**

1989 The refinement was necessary to ensure unified terminology usage of SFRs.

1990 FIA_UAU.1/PACE_EAC2PP
 1991 Timing of authentication

1992 Hierarchical to: No other components

1993 Dependencies: [FIA_UID.1 Timing of identification]: fulfilled by
 1994 FIA_UID.1/PACE_EAC2PP

1995 FIA_UAU.1.1/PACE_EAC2PP

1996 The TSF shall allow:

- 1997 1. to establish a communication channel,
- 1998 2. carrying out the PACE protocol according to [17],
- 1999 3. to read the Initialization Data if it is not disabled by TSF according to
 2000 **FMT_MTD.1/INI_DISFMT_MTD.1/INI_DIS_EAC2PP,**
- 2001 4. none¹⁰⁵

2002 on behalf of the user to be performed before the user is authenticated.

2003 FIA_UAU.1.2/PACE_EAC2PP

¹⁰⁵ [assignment: list of TSF-mediated actions]

2004 The TSF shall require each user to be successfully authenticated before allowing any other
 2005 TSF-mediated actions on behalf of that user.

2006 **46. Application note (taken from [6], application note 24)**

2007 If PACE has been successfully performed, secure messaging is started using the derived
 2008 session keys (PACE- K_{MAC} , PACE- K_{Enc}), cf. FTP_ITC.1/PACE_EAC2PP. 44. Application note
 2009 (taken from [6], application note 23) also applies here.

2010 **47. Application note (from ST author)**

2011 The refinement was necessary to ensure unified terminology usage of SFRs.

2012 FIA_UAU.1/EAC2_Terminal_EAC2PP
 2013 Timing of authentication

2014 Hierarchical to: No other components

2015 Dependencies: [FIA_UID.1 Timing of identification]: fulfilled by
 2016 FIA_UAU.1/EAC2_Terminal_EAC2PP

2017 FIA_UAU.1.1/EAC2_Terminal_EAC2PP

2018 The TSF shall allow:

- 2019 1. to establish a communication channel,
- 2020 2. carrying out the PACE protocol according to [17],
- 2021 3. to read the Initialization Data if it is not disabled by TSF according to
 2022 ~~FMT_MTD.1/INI_DIS~~FMT_MTD.1/INI_DIS_EAC2PP
- 2023 4. carrying out the Terminal Authentication protocol 2 according to [17]¹⁰⁶

2024 on behalf of the user to be performed before the user is authenticated.

2025 FIA_UAU.1.2/EAC2_Terminal_EAC2PP

2026 The TSF shall require each user to be successfully authenticated before allowing any other
 2027 TSF-mediated actions on behalf of that user.

2028 **48. Application note (taken from [6], application note 25)**

2029 The user authenticated after a successful run of TA2 is an EAC2 terminal. The authenticated
 2030 terminal will immediately perform Chip Authentication 2 as required by
 2031 FIA_API.1/CA_EAC2PP using, amongst other, Comp(ephem-PK_{PCD}-TA) from the
 2032 accomplished TA2. Note that Passive Authentication using SO_C is considered to be part of
 2033 CA2 within this ST.

¹⁰⁶ [assignment: list of TSF-mediated actions]

2034 **49. Application note (from ST author)**

2035 The refinement was necessary to ensure unified terminology usage of SFRs.

2036 FIA_UAU.4/PACE_EAC2PP

2037 Single-use authentication of the Terminals by the TOE

2038 Hierarchical to: No other components

2039 Dependencies: No dependencies

2040 FIA_UAU.4.1/PACE_EAC2PP

2041 The TSF shall prevent reuse of authentication data related to:

- 2042 1. PACE protocol according to [17].
- 2043 2. Authentication Mechanism based on AES¹⁰⁷
- 2044 3. Terminal Authentication 2 protocol according to [17].¹⁰⁸
- 2045 4. none¹⁰⁹

2046 **50. Application note (taken from [6], application note 26)**

2047 For PACE, the TOE randomly selects an almost uniformly distributed nonce of 128 bit length.
 2048 The [6] supports a key derivation function based on AES; see [17]. For TA2, the TOE randomly
 2049 selects a nonce r_{PICC} of 64 bit length, see [17]. This SFR extends FIA_UAU.4/PACE from [13]
 2050 by assigning the authentication mechanism Terminal Authentication 2.

2051 FIA_UAU.5/PACE_EAC2PP

2052 Multiple authentication mechanisms

2053 Hierarchical to: No other components

2054 Dependencies: No dependencies

2055 FIA_UAU.5.1/PACE_EAC2PP

2056 The TSF shall provide

- 2057 1. PACE protocol according to [17].
- 2058 2. Passive Authentication according to [8]
- 2059 3. Secure messaging in **MAC-ENC** mode according to [18]
- 2060 4. Symmetric Authentication Mechanism based on TDES and AES¹¹⁰¹¹

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

¹⁰⁸ [assignment: identified authentication mechanism(s)]

¹⁰⁹ [assignment: identified authentication mechanism(s)]

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

¹¹¹ [selection: AES or other approved algorithms]

2061 5. Terminal Authentication 2 protocol according to [17].

2062 6. Chip Authentication 2 according to [17]¹¹²¹¹³

2063 7. none¹¹⁴

2064 to support user authentication.

2065 FIA_UAU.5.2/PACE_EAC2PP

2066 The TSF shall authenticate any user's claimed identity according to the following rules:

2067 1. Having successfully run the PACE protocol the TOE accepts only received
 2068 commands with correct message authentication codes sent by secure messaging
 2069 with the key agreed with the terminal by the PACE protocol.

2070 2. The TOE accepts the authentication attempt as Personalization Agent by
 2071 Symmetric Authentication (Device authentication) according to [30]¹¹⁵

2072 3. The TOE accepts the authentication attempt by means of the Terminal
 2073 Authentication 2 protocol, only if (i) the terminal presents its static public key PK_{PCD}
 2074 and the key is successfully verifiable up to the CVCA and (ii) the terminal uses the
 2075 PICC identifier $IDP_{PICC} = \text{Comp}(\text{ephem-PK}_{PICC}\text{-PACE})$ calculated during, and the
 2076 secure messaging established by the, current PACE authentication.

2077 4. Having successfully run Chip Authentication 2, the TOE accepts only received
 2078 commands with correct message authentication codes sent by secure messaging
 2079 with the key agreed with the terminal by Chip Authentication 2.¹¹⁶

2080 5. none¹¹⁷

2081 **51. Application note (taken from [6], application note 27)**

2082 Refinement of FIA_UAU.5.2/PACE_EAC2PP, since here PACE must adhere to [17] and [18],
 2083 cf. 9. Application note (taken from [6], application note 10). Since the formulation "MAC-ENC
 2084 mode" is slightly ambiguous (there is only one secure messaging mode relevant both in [13]
 2085 and here, and it is actually the same in both references), it is removed here by refinement in
 2086 the third bullet point of FIA_UAU.5.1/PACE_EAC2PP.

2087 Remark: Note that 5. and 6. in FIA_UAU.5.1/PACE_EAC2PP and 3. and 4. of
 2088 FIA_UAU.5.2/PACE_EAC2PP are additional assignments (using the open assignment
 2089 operation) compared to [13].

2090 **52. Application note (from ST author)**

¹¹² Passive Authentication using SO_C is considered to be part of CA2 within this ST.

¹¹³ [assignment: *list of multiple authentication mechanisms*]

¹¹⁴ [assignment: *list of multiple authentication mechanisms*]

¹¹⁵ [selection: *the Authentication Mechanism with Personalization Agent Key(s)*]

¹¹⁶ [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

¹¹⁷ [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

- 2091 Symmetric Authentication Mechanism implemented according to [30].
- 2092 FIA_UAU.6/CA_EAC2PP
 2093 Re-authenticating of Terminal by the TOE
- 2094 Hierarchical to: No other components
- 2095 Dependencies: No dependencies
- 2096 FIA_UAU.6.1/CA_EAC2PP
- 2097 The TSF shall re-authenticate the user under the conditions each command sent to the
 2098 TOE after a successful run of Chip Authentication 2 shall be verified as being sent by the
 2099 EAC2 terminal¹¹⁸.
- 2100 FIA_AFL.1/PACE_EAC2PP
 2101 Authentication failure handling – PACE authentication using non-blocking authorisation data
- 2102 Hierarchical to: No other components
- 2103 Dependencies: [FIA_UAU.1 Timing of authentication]: fulfilled by
 2104 FIA_UAU.1/PACE_EAC2PP
- 2105 FIA_AFL.1.1/PACE_EAC2PP
- 2106 The TSF shall detect when an administrator configurable positive integer number within
 2107 [1-127]¹¹⁹ unsuccessful authentication attempt occurs related to authentication attempts
 2108 using the PACE password as shared password.¹²⁰
- 2109 FIA_AFL.1.2/PACE_EAC2PP
- 2110 When the defined number of unsuccessful authentication attempts has been met¹²¹, the
 2111 TSF shall delay each following authentication attempt until the next successful
 2112 authentication.¹²²
- 2113 **53. Application note (from ST author)**
- 2114 In line with [6] the shared password for PACE can be CAN, MRZ, PIN and PUK. The specific
 2115 case of PIN is detailed in FIA_AFL.1/Suspend_PIN_EAC2PP and

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

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

¹²⁰ [assignment: list of authentication events]

¹²¹ [selection: met ,surpassed]

¹²² [assignment: list of actions]

2116 FIA_AFL.1/Block_PIN_EAC2PP and furthermore 39. Application note (taken from [6],
 2117 application note 19).

2118 FIA_UAU.6/PACE_EAC2PP
 2119 Re-authenticating of Terminal by the TOE

2120 Hierarchical to: No other components

2121 Dependencies: No dependencies

2122 FIA_UAU.6.1/PACE_EAC2PP

2123 The TSF shall re-authenticate the user under the conditions each command sent to the
 2124 TOE after successful run of the PACE protocol shall be verified as being sent by the PACE
 2125 terminal.¹²³

2126 *6.1.2.2. SFRs for EAC1-protected data*

- 2127 • FIA_UID.1/PACE_EAC1PP
- 2128 • FIA_UAU.1/PACE_EAC1PP
- 2129 • FIA_UAU.4/PACE_EAC1PP
- 2130 • FIA_UAU.5/PACE_EAC1PP
- 2131 • FIA_UAU.6/PACE_EAC1PP

2132 (equivalent to FIA_UAU.6/PACE_EAC2PP, but listed here for the sake of completeness)

- 2133 • FIA_UAU.6/EAC_EAC1PP
- 2134 • FIA_API.1/EAC1PP
- 2135 • FIA_AFL.1/PACE_EAC1PP

2136 (equivalent to FIA_AFL.1/PACE_EAC2PP, but listed here for the sake of completeness)

2137 FIA_UID.1/PACE_EAC1PP
 2138 Timing of identification

2139 Hierarchical to: No other components

2140 Dependencies: No dependencies

2141 FIA_UID.1.1/PACE_EAC1PP

2142 The TSF shall allow:

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

- 2143 1. to establish the communication channel.
- 2144 2. carrying out the PACE Protocol according to [7].
- 2145 3. to read the Initialization Data if it is not disabled by TSF according to
- 2146 ~~FMT_MTD.1/INI_DIS-FMT_MTD.1/INI_DIS~~ EAC1PP
- 2147 4. to carry out the Chip Authentication Protocol v.1 according to [16] or the Chip
- 2148 **Authentication mapping (PACE-CAM) according to [9].**
- 2149 5. to carry out the Terminal Authentication Protocol v.1 according to [16] resp.
- 2150 **according to [9] if PACE-CAM is used.**¹²⁴
- 2151 6. none¹²⁵.

2152 on behalf of the user to be performed before the user is identified.

2153 FIA_UID.1.2/PACE_EAC1PP

2154 The TSF shall require each user to be successfully identified before allowing any other

2155 TSF-mediated actions on behalf of that user.

2156 **54. Application note (from ST author)**

2157 The SFR is refined here in order for the TSF to *additionally* provide the PACE-CAM protocol

2158 by referencing [9]. PACE-CAM combines PACE and Chip Authentication 1 for faster execution

2159 times. Hence, a TOE meeting the original requirement also meets the refined requirement.

2160 **55. Application note (taken from [5], application note 20)**

2161 The SFR FIA_UID.1/PACE in [5] covers the definition in [13] and extends it by EAC aspect 4.

2162 This extension does not conflict with the strict conformance to [13].

2163 **56. Application note (taken from [5], application note 21)**

2164 In the Phase 2 “Manufacturing” the Manufacturer is the only user role known to the TOE which

2165 writes the Initialization Data and/or Pre-personalisation Data in the audit records of the IC. The

2166 electronic document manufacturer may create the user role Personalisation Agent for transition

2167 from Phase 2 to Phase 3 “Personalisation of the Electronic Document”. The users in role

2168 Personalisation Agent identify themselves by means of selecting the authentication key. After

2169 personalisation in the Phase 3 the PACE domain parameters, the Chip Authentication data

2170 and Terminal Authentication Reference Data are written into the TOE. The Inspection System

2171 is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE

2172 protocol, to gain access to the Chip Authentication Reference Data and to run the Chip

2173 Authentication Protocol Version 1. After successful authentication of the chip the terminal may

2174 identify itself as (i) EAC1 terminal by selection of the templates for the Terminal Authentication

2175 Protocol Version 1 or (ii) if necessary and available by authentication as Personalisation Agent

2176 (using the Personalisation Agent Key).

2177 **57. Application note (taken from [5], application note 22)**

¹²⁴ [assignment: list of TSF-mediated actions]

¹²⁵ [assignment: list of TSF-mediated actions]

2178 User identified after a successfully performed PACE protocol is a terminal. Please note that
 2179 neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either
 2180 the electronic document holder itself or an authorised other person or device (PACE terminal).

2181 **58. Application note (taken from [5], application note 23)**

2182 In the life-cycle phase 'Manufacturing' the Manufacturer is the only user role known to the TOE.
 2183 The Manufacturer writes the Initialisation Data and/or Pre-personalisation Data in the audit
 2184 records of the IC.

2185 Please note that a Personalisation Agent acts on behalf of the electronic document Issuer
 2186 under his and CSCA and DS policies. Hence, they define authentication procedure(s) for
 2187 Personalisation Agents. The TOE must functionally support these authentication procedures
 2188 being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1.
 2189 The TOE assumes the user role 'Personalisation Agent', when a terminal proves the respective
 2190 Terminal Authorisation Level as defined by the related policy (policies).

2191 **59. Application note (from ST author)**

2192 The refinement was necessary to ensure unified terminology usage of SFRs.

2193 FIA_UAU.1/PACE_EAC1PP
 2194 Timing of authentication

2195 Hierarchical to: No other components

2196 Dependencies: FIA_UID.1 Timing of identification fulfilled by
 2197 FIA_UID.1/PACE_EAC1PP

2198 FIA_UAU.1.1/PACE_EAC1PP

2199 The TSF shall allow:

- 2200 1. to establish the communication channel,
- 2201 2. carrying out the PACE Protocol according to [7],
- 2202 3. to read the Initialization Data if it is not disabled by TSF according to
 2203 **FMT_MTD.1/INI DIS-FMT MTD.1/INI DIS EAC1PP,**
- 2204 4. to identify themselves by selection of the authentication key
- 2205 5. to carry out the Chip Authentication Protocol Version 1 according to [16]
- 2206 6. to carry out the Terminal Authentication Protocol Version 1 according to [16]¹²⁶
- 2207 7. to carry out the Active Authentication Mechanism according to [9]¹²⁷

2208 on behalf of the user to be performed before the user is authenticated.

¹²⁶ [assignment: list of TSF-mediated actions]

¹²⁷ [assignment: list of TSF-mediated actions]

2209 FIA_UAU.1.2/PACE_EAC1PP

2210 The TSF shall require each user to be successfully authenticated before allowing any other
 2211 TSF-mediated actions on behalf of that user.

2212 **60. Application note (taken from [5], application note 24)**

2213 The SFR FIA_UAU.1/PACE_EAC1PP in the current ST covers the definition in [13] and
 2214 extends it by EAC aspect 5. This extension does not conflict with the strict conformance to
 2215 [13].

2216 **61. Application note (taken from [5], application note 25)**

2217 The user authenticated after a successfully performed PACE protocol is a terminal. Please
 2218 note that neither CAN nor MRZ effectively represent secrets but are restricted revealable; i.e.
 2219 it is either the electronic document holder itself or an authorised another person or device
 2220 (PACE terminal).

2221 If PACE was successfully performed, secure messaging is started using the derived session
 2222 keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE_EAC1PP.

2223 **62. Application note (from ST author)**

2224 The refinement was necessary to ensure unified terminology usage of SFRs.

2225 FIA_UAU.4/PACE_EAC1PP

2226 Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

2227 Hierarchical to: No other components

2228 Dependencies: No dependencies

2229 FIA_UAU.4.1/PACE_EAC1PP

2230 The TSF shall prevent reuse of authentication data related to

- 2231 1. PACE Protocol according to [7],
- 2232 2. Authentication Mechanism based on Triple-DES or AES¹²⁸
- 2233 3. Terminal Authentication Protocol v.1 according to [16].¹²⁹
- 2234 4. **Active Authentication protocol according to [7], [9]**

2235 **63. Application note (taken from [5], application note 26)**

2236 The SFR FIA_UAU.4.1/PACE_EAC1PP in the current ST covers the definition in [13] and
 2237 extends it by the EAC aspect 3. This extension does not conflict with the strict conformance to
 2238 [13]. The generation of random numbers (random nonce) used for the authentication protocol

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

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

2239 (PACE) and Terminal Authentication as required by FIA_UAU.4/PACE_EAC1PP is required
 2240 by FCS_RND.1 from [13].

2241 **64. Application note (taken from [5], application note 27)**

2242 The authentication mechanisms may use either a challenge freshly and randomly generated
 2243 by the TOE to prevent reuse of a response generated by a terminal in a successful
 2244 authentication attempt. However, the authentication of Personalisation Agent may rely on other
 2245 mechanisms ensuring protection against replay attacks, such as the use of an internal counter
 2246 as a diversifier.

2247 **65. Application note (ST author)**

2248 The refinement was necessary because the authentication data (nonce) is must not be reused
 2249 during Active Authentication protocol according to [9].

2250 FIA_UAU.5/PACE_EAC1PP
 2251 Multiple authentication mechanisms

2252 Hierarchical to: No other components

2253 Dependencies: No dependencies

2254 FIA_UAU.5.1/PACE_EAC1PP

2255 The TSF shall provide

- 2256 1. PACE Protocol according to [7] and PACE-CAM protocol according to [9]
- 2257 2. Passive Authentication according to [8]
- 2258 3. Secure messaging in MAC-ENC mode according to [7].
- 2259 4. Symmetric Authentication Mechanism based on Triple-DES or AES¹³⁰
- 2260 5. Terminal Authentication Protocol v.1 according to [16].¹³¹

2261 to support user authentication

2262 FIA_UAU.5.2/PACE_EAC1PP

2263 The TSF shall authenticate any user's claimed identity according to the following rules:

- 2264 1. Having successfully run the PACE protocol the TOE accepts only received
- 2265 commands with correct message authentication code sent by means of secure
- 2266 messaging with the key agreed with the terminal by means of the PACE protocol.

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

¹³¹ [assignment: list of multiple authentication mechanism]

- 2267 2. The TOE accepts the authentication attempt as Personalisation Agent by the
- 2268 Symmetric Authentication (Device authentication) according to [30]¹³²
- 2269 3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only
- 2270 received commands with correct message authentication code sent by means of
- 2271 secure messaging with key agreed with the terminal by means of the Chip
- 2272 Authentication Mechanism v1.
- 2273 4. The TOE accepts the authentication attempt by means of the Terminal
- 2274 Authentication Protocol v.1 only if the terminal uses the public key presented during
- 2275 the Chip Authentication Protocol v.1 and the secure messaging established by the
- 2276 Chip Authentication Mechanism v.1. **or if the terminal uses the public key**
- 2277 **presented during PACE-CAM and the secure messaging established during**
- 2278 **PACE.**¹³³
- 2279 5. none¹³⁴

2280 **66. Application note (from ST author)**

2281 The SFR is refined here in order for the TSF to additionally provide the PACE-CAM protocol
 2282 by referencing [9]. PACE-CAM combines PACE and Chip Authentication 1 for faster execution
 2283 times. Hence, a TOE meeting the original requirement also meets the refined requirement.

2284 **67. Application note (taken from [5], application note 28)**

2285 The SFR FIA_UAU.5.1/PACE_EAC1PP in the current ST covers the definition in [13] and
 2286 extends it by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE_EAC1PP in the current
 2287 ST covers the definition in [13] and extends it by EAC aspects 2), 3), 4) and 5). These
 2288 extensions do not conflict with the strict conformance to [13].

2289 **FIA_UAU.6/EAC_EAC1PP**

2290 **Re-authenticating – Re-authenticating of Terminal by the TOE**

2291 Hierarchical to: No other components

2292 Dependencies: No dependencies

2293 **FIA_UAU.6.1/EAC_EAC1PP**

2294 The TSF shall re-authenticate the user under the conditions each command sent to the
 2295 TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as
 2296 being sent by the Inspection System.¹³⁵

¹³² [selection: *the Authentication Mechanism with Personalisation Agent Key(s)*]

¹³³ [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

¹³⁴ [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

¹³⁵ [assignment: *list of conditions under which re-authentication is required*]

2297 **68. Application note (taken from [5], application note 29)**

2298 The Password Authenticated Connection Establishment and the Chip Authentication Protocol
2299 specified in [8] include secure messaging for all commands exchanged after successful
2300 authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC
2301 mode each command based on a corresponding MAC algorithm whether it was sent by the
2302 successfully authenticated terminal (see FCS_COP.1/CA_MAC_EAC1PP for further details).
2303 The TOE does not execute any command with incorrect message authentication code.

2304 Therefore the TOE re-authenticates the user for each received command and accepts only
2305 those commands received from the previously authenticated user.

2306 FIA_API.1/EAC1PP
2307 Authentication Proof of Identity

2308 Hierarchical to: No other components

2309 Dependencies: No dependencies

2310 FIA_API.1.1/EAC1PP

2311 The TSF shall provide a Chip Authentication Protocol Version 1 according to [16]¹³⁶ to
2312 prove the identity of the TOE.¹³⁷

2313 **69. Application note (taken from [5], application note 30)**

2314 This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in
2315 [16]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol
2316 (DH or ECDH) and two session keys for secure messaging in ENC_MAC mode according to
2317 [8]. The terminal verifies by means of secure messaging whether the electronic document's
2318 chip was able or not to run his protocol properly using its Chip Authentication Private Key
2319 corresponding to the Chip Authentication Key (EF.DG14).

2320 The following SFR is newly defined in this ST and addresses the PACE-CAM protocol.

2321 FIA_API.1/PACE_CAM
2322 Authentication Proof of Identity

2323 Hierarchical to: No other components

2324 Dependencies: No dependencies

2325 FIA_API.1.1/PACE_CAM

2326 The TSF shall provide a protocol PACE-CAM [9]¹³⁸ to prove the identity of the TOE.¹³⁹

¹³⁶ [assignment: *authentication mechanism*]

¹³⁷ [assignment: *authorized user or role*]

¹³⁸ [assignment: *authentication mechanism*]

¹³⁹ [assignment: *authorized user or role, or of the TOE itself*]

2327 The following SFR is newly defined in this ST and addresses the Active Authentication
 2328 protocol:

2329 FIA_API.1/AA
 2330 Authentication Proof of Identity

2331 Hierarchical to: No other components

2332 Dependencies: No dependencies

2333 FIA_API.1.1/AA

2334 The TSF shall provide a Active Authentication protocol according to [7] [9]¹⁴⁰ to prove the
 2335 identity of the TOE.¹⁴¹

2336 The following SFRs are imported due to claiming [14]. They concern access mechanisms for
 2337 an eSign application, if available.

- 2338 • FIA_UID.1/SSCDPP
- 2339 • FIA_AFL.1/SSCDPP

2340 FIA_UID.1/SSCDPP
 2341 Timing of identification

2342 Hierarchical to: No other components

2343 Dependencies: No dependencies

2344 FIA_UID.1.1/SSCDPP

2345 The TSF shall allow

- 2346 1. Self-test according to ~~FPT TST.1~~ FPT TST.1/SSCDPP.
- 2347 2. none¹⁴²

2348 on behalf of the user to be performed before the user is identified

2349 FIA_UID.1.2/SSCDPP

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

- 2350 The TSF shall require each user to be successfully identified before allowing any other
 2351 TSF-mediated actions on behalf of that user.
- 2352 **70. Application note (taken from [14], application note 11)**
- 2353 Applied.
- 2354 **71. Application note (from ST author)**
- 2355 The refinement was necessary to ensure unified terminology usage of SFRs.
- 2356 FIA_AFL.1/SSCDPP
 2357 Authentication failure handling
- 2358 Hierarchical to: No other components
- 2359 Dependencies: FIA_UAU.1 Timing of Authentication fulfilled by
 2360 FIA_UAU.1/SSCDPP
- 2361 FIA_AFL.1.1/SSCDPP
- 2362 The TSF shall detect when an administrator configurable positive integer within 3-15¹⁴³
 2363 unsuccessful authentication attempts occur related to consecutive failed authentication
 2364 attempts.¹⁴⁴
- 2365 FIA_AFL.1.2/SSCDPP
- 2366 When the defined number of unsuccessful authentication attempts has been met¹⁴⁵, the
 2367 TSF shall block RAD¹⁴⁶.
- 2368 **72. Application note (taken from [14], application note 13)**
- 2369 Applied
- 2370 **6.1.2.3. SFRs for eSign-applications**
- 2371 FIA_UAU.1/SSCDPP
 2372 Timing of authentication
- 2373 Hierarchical to: No other components

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

¹⁴⁴ [assignment: list of authentication events]

¹⁴⁵ [selection: met ,surpassed]

¹⁴⁶ [assignment: list of actions]

2374 Dependencies: FIA_UID.1 Timing of identification: fulfilled by
 2375 FIA_UID.1/SSCDPP

2376 FIA_UAU.1.1/SSCDPP

2377 The TSF shall allow

- 2378 1. self test according to ~~FPT TST.1/SSCD~~ **FPT TST.1/SSCDPP**,
- 2379 2. identification of the user by means of TSF required by ~~FIA UID.1/SSCD~~
 2380 **FIA UID.1/SSCDPP**,
- 2381 3. establishing a trusted channel between CGA and the TOE by means of TSF
 2382 required by ~~FPT ITC.1/CA EAC2~~ **FTP ITC.1/CA EAC2PP**,
- 2383 4. establishing a trusted channel between HID and the TOE by means of TSF
 2384 required by ~~FPT ITC.1/CA EAC2~~ **FTP ITC.1/CA EAC2PP**,
- 2385 5. none¹⁴⁷

2386 on behalf of the user to be performed before the user is authenticated.

2387 FIA_UAU.1.2/SSCDPP

2388 The TSF shall require each user to be successfully authenticated before allowing any other
 2389 TSF-mediated actions on behalf of that user.

2390 **73. Application note (from ST author)**

2391 The refinement was necessary to ensure unified terminology usage of SFRs.

2392 **6.1.3. Class FDP**

2393 Multiple iterations of FDP_ACF.1 exist from imported PPs to define the access control SFPs
 2394 for (common) user data, EAC1-protected user data, and EAC2-protected user data. The
 2395 access control SFPs defined in FDP_ACF.1/EAC1PP from [5] and FDP_ACF.1/EAC2PP from
 2396 [6] are unified in [20] to one single FDP_ACF.1/TRM, whereas the several iterations of
 2397 FDP_ACF.1 from [14] stand separate. [20] takes FDP_ACF.1/EAC2PP as a base definition of
 2398 functional elements, and it is refined in a way that it is compatible with FDP_ACF.1/EAC1PP.
 2399 Hence highlighting refers to changes w.r.t. to FDP_ACF.1/EAC2PP. In the application note
 2400 below, how FDP_ACF.1/EAC1PP is covered as well is explained.

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

2401 Concerning FDP_ACF.1/TRM in [20] and the several iterations FDP_ACF.1 from [14], [20]
 2402 remarks that FDP_ACF.1/TRM also concerns data and objects for signature generation. Note
 2403 however, that FDP_ACF.1/TRM requires that prior to granting access to the signature
 2404 application, in which the access controls defined in [14] apply, an EAC2 terminal and the
 2405 Electronic Document Holder need to be authenticated. Hence, no inconsistency exists.

2406 FDP_ACF.1/TRM
 2407 Security attribute based access control – Terminal Access

2408 Hierarchical to: No other components

2409 Dependencies: FDP_ACC.1 Subset access control fulfilled by
 2410 FDP_ACC.1/TRM_EAC1PP and
 2411 FDP_ACC.1/TRM_EAC2PP

2412 FMT_MSA.3 Static attribute initialization not fulfilled, but
 2413 **justified:**

2414 The access control TSF according to FDP_ACF.1/TRM
 2415 uses security attributes having been defined during the
 2416 personalization and fixed over the whole life time of the
 2417 TOE. No management of these security attributes (i.e.
 2418 SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

2419 FDP_ACF.1.1/TRM

2420 The TSF shall enforce the Access Control SFP¹⁴⁸ to objects based on the following:

- 2421 1) Subjects:
- 2422 a) Terminal,
- 2423 b) PACE terminal,
- 2424 c) EAC2 terminal Authentication Terminal and Signature Terminal according to
 2425 [17]¹⁴⁹,
- 2426 d) EAC1 terminal.¹⁵⁰
- 2427 2) Objects:

¹⁴⁸ [assignment: access control SFP]

¹⁴⁹ [assignment: list of EAC2 terminal types]

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

- 2428 a) all user data stored in the TOE; including sensitive **EAC1-protected user**
 2429 **data, and sensitive EAC2-protected** user data.
- 2430 b) all TOE intrinsic secret (cryptographic) data
- 2431 3) Security attributes:
- 2432 a) Terminal Authorization Level (access rights)
- 2433 b) Authentication status of the Electronic Document Holder as a signatory (if an
 2434 eSign application is included).¹⁵¹¹⁵²
- 2435 FDP_ACF.1.2/TRM
- 2436 The TSF shall enforce the following rules to determine if an operation among controlled
 2437 subjects and controlled objects is allowed:
- 2438 A PACE terminal is allowed to read data objects from FDP_ACF.1/TRM after successful
 2439 PACE authentication according to [17] and/or [7], as required by **FIA_UAU.1/PACE**
 2440 **FIA_UAU.1/PACE_EAC2PP** or **FIA_UAU.1/PACE_EAC1PP**.¹⁵³
- 2441 FDP_ACF.1.3/TRM
- 2442 The TSF shall explicitly authorize access of subjects to objects based on the following
 2443 additional rules: none.¹⁵⁴
- 2444 FDP_ACF.1.4/TRM
- 2445 The TSF shall explicitly deny access of subjects to objects based on the following
 2446 additional rules:
- 2447 1. Any terminal not being ~~authenticated~~ as a PACE terminal or an EAC2 terminal or
 2448 an **EAC1 terminal** is not allowed to read, to write, to modify, or to use any user
 2449 data stored on the electronic document.¹⁵⁵
- 2450 2. Terminals not using secure messaging are not allowed to read, write, modify, or
 2451 use any data stored on the electronic document.

¹⁵¹ [assignment: list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or name groups of SFP-relevant security attributes] (added using open assignment of [6])

¹⁵² [assignment: list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or name groups of SFP-relevant security attributes] (all bullets in FDP_ACF.1.1/TRM w.r.t. [2])

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

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

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

- 2452 3. No subject is allowed to read ‘Electronic Document Communication Establishment
 2453 Authorization Data’ stored on the electronic document
- 2454 4. No subject is allowed to write or modify ‘Secret Electronic Document Holder
 2455 Authentication Data’ stored on the electronic document, except for PACE terminals
 2456 or EAC2 terminals executing PIN management based on the following rules:
- 2457 1. CAN change
 2458 2. Change PIN
 2459 3. Resume PIN
 2460 4. Unblock PIN
 2461 5. Activate PIN
 2462 6. Deactivate PIN according to [17].¹⁵⁶
- 2463 5. No subject is allowed to read, write, modify, or use the private Restricted
 2464 Identification key(s) and Chip Authentication key(s) stored on the electronic
 2465 document.
- 2466 6. Reading, modifying, writing, or using Sensitive User Data that are protected only
 2467 by EAC2, is allowed only to EAC2 terminals using the following mechanism:
- 2468 The TOE applies the EAC2 protocol (cf. **FIA_UAU.5**
 2469 **FIA_UAU.5/PACE_EAC2PP**) to determine access rights of the terminal
 2470 according to [17]. To determine the effective authorization of a terminal, the
 2471 chip must calculate a bitwise Boolean ‘and’ of the relative authorization
 2472 contained in the CHAT of the Terminal Certificate, the referenced DV
 2473 Certificate, and the referenced CVCA Certificate, and additionally the confined
 2474 authorization sent as part of PACE. Based on that effective authorization and
 2475 the terminal type drawn from the CHAT of the Terminal Certificate, the TOE
 2476 shall grant the right to read, modify or write Sensitive User Data, or perform
 2477 operations using these Sensitive User Data.
- 2478 7. No subject is allowed to read, write, modify or use the data objects 2b) of
 2479 FDP ACF.1/TRM.
- 2480 8. No subject is allowed to read Sensitive User Data that are protected only by EAC1,
 2481 except an EAC1 terminal (OID inspection system) after EAC1, cf.
 2482 **FIA_UAU.1/EAC1 FIA_UAU.1/PACE_EAC1PP**, that has a corresponding relative
 2483 authorization level. This includes in particular EAC1-protected user data DG3 and
 2484 DG4 from an ICAO-compliant ePass application, cf. [16] and [8].

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

2485 9. If Sensitive User Data is protected both by EAC1 and EAC2, no subject is allowed
2486 to read those data except EAC1 terminals or EAC2 terminals that access these
2487 data according to rule 6 or rule 8 above.

2488 10. Nobody is allowed to read the private signature key(s).¹⁵⁷

2489 **74. Application note (from ST author)**

2490 The [20] uses the 'Electronic Document Communication Establishment Authorization Data'
2491 expression in 3.1.1.2 Secondary Assets and "Communication Establishment Authorization
2492 Data" in FDP_ACF.1.4/TRM 3. In order to provide consistency in our ST, we use only the
2493 Electronic Document Communication Establishment Authorization Data.

2494 **75. Application note (taken from [20], application note 11)**

2495 The above definition is based on FDP_ACF.1/TRM_EAC2PP. We argue that it covers
2496 FDP_ACF.1/TRM_EAC1PP as well. Subject 1b and 1d are renamed here from
2497 FDP_ACF.1.1/TRM_EAC1PP according to Table 1 Objects in 2), in particular the term EAC1-
2498 protected user data, subsume all those explicitly enumerated in FDP_ACF.1.1/TRM_EAC1PP.
2499 Also, the security attribute 3a) Terminal Authorization Level here subsumes the explicitly
2500 enumerated attributes 3a) and 3b) of FDP_ACF.1.1/TRM_EAC1PP, but are semantically the
2501 same. Since in addition EAC2 protected data are stored in the TOE of this ST, additional
2502 subjects, objects and security attributes are listed here. However, since they apply to data with
2503 a different protection mechanism (EAC2), strict conformance is not violated.

2504 FDP_ACF.1.2/TRM uses the renaming of Table 1 , and references in addition [17]. However
2505 the references are compatible as justified in [6], yet both are mentioned here since [17] is the
2506 primary norm for an eID application, whereas [7] is normative for an ICAO compliant ePass
2507 application. Investigating the references reveals that access to data objects defined in
2508 FDP_ACF.1.1/TRM must be granted if these data are neither EAC1-protected, nor EAC2-
2509 protected.

2510 FDP_ACF.1.3/TRM is the same as in FDP_ACF.1.3/TRM_EAC2PP.

2511 References are changed in FDP_ACF.1.2/TRM_EAC1PP. It is already justified in [6] that
2512 definitions in [17] and [8] are compatible.

2513 FDP_ACF.1.3/TRM is taken over from [5] and [6] (same formulation in both).

2514 Rules 1 and 2 of FDP_ACF.1.4/TRM_EAC1PP in [5] are covered by their counterparts rule 1
2515 and rule 2 here. Rules 3 and 4, and rule 6 of FDP_ACF.1.4/TRM_EAC1PP in [5] are combined
2516 here to rule 8, where terminals need the corresponding CHAT to read data groups. Rule 5 of
2517 [5] is here equivalent to rule 7. None of this conflict with strict conformance to [5]. Note that
2518 adding additional rules compared to FDP_ACF.1.4/TRM_EAC1PP here can never violate strict
2519 conformance, as these are rules that explicitly deny access of subjects to objects. Hence
2520 security is always increased.

2521 The above definition also covers FDP_ACF.1.1/TRM_EAC2PP and extends it by additional
2522 subjects and objects. Sensitive User Data in the definition of FDP_ACF.1.1/TRM_EAC2PP are
2523 here EAC2-protected Sensitive User Data. EAC1-protected data are added here by

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

2524 refinement. Since the protection level and mechanisms w.r.t. to EAC2-protected data do not
2525 change, strict conformance is not violated.

2526 FDP_ACF.1.2/TRM_EAC2PP and FDP_ACF.1.3/TRM_EAC2PP are equivalent to the current
2527 definition.

2528 Rules 8, 9 and 10 are added here by open assignment from [6]. None of these conflicts with
2529 strict conformance.

2530 The dependency of this SFR is met by FDP_ACC.1/TRM_EAC1PP and
2531 FDP_ACC.1/TRM_EAC2PP. Note that the SFR in [5] applies the assignment operation,
2532 whereas in [6] (by referencing [13]) the assignment is left open. Hence, they are compatible.
2533 We remark that in order to restrict the access to user data as defined in the SFR
2534 FDP_ACC.1/TRM_EAC1PP, clearly access to objects 2b) of FDP_ACF.1.1/TRM must be
2535 restricted as well according to the SFP, otherwise access to user data is impossible to enforce.

2536 [76. Application note \(from ST author\)](#)

2537 The refinements were necessary to ensure unified terminology usage of SFRs.

2538 The following SFRs are imported due to claiming [6]. They concern access control mechanisms
2539 related to EAC2-protected data.

2540

- **FDP_ACC.1/TRM_EAC2PP**

2541 This SFR is equivalent to/covered by **FDP_ACC.1/TRM_EAC1PP**; cf the 75. Application note
2542 (taken from [20], application note 11).

2543

- **FDP_ACF.1/TRM_EAC2PP**

2544 This is SFR is equivalent to/covered by **FDP_ACF.1/TRM**.

2545

- **FDP_RIP.1/EAC2PP**

2546

- **FDP_UCT.1/TRM_EAC2PP**

2547

- **FDP_UIT.1/TRM_EAC2PP**

2548 FDP_ACC.1/TRM_EAC2PP
2549 Subset access control – Terminal Access

2550 Hierarchical to: No other components

2551 Dependencies: FDP_ACF.1 Security attribute based access control:
2552 fulfilled by FDP_ACF.1/TRM

2553 FDP_ACC.1.1/TRM_EAC2PP

2554 The TSF shall enforce the Access Control SFP¹⁵⁸ on terminals gaining access to the User
 2555 Data stored in the ~~travel document~~ **electronic document**¹⁵⁹ and none¹⁶⁰.

2556 **77. Application note (taken from [20])**

2557 This SFR is equivalent to/covered by FDP_ACC.1/TRM_EAC1PP; cf.75. Application note
 2558 (taken from [20], application note 11).

2559 **78. Application note (from ST author)**

2560 The refinement was necessary to ensure unified terminology usage as described in Table 1
 2561 Overview of identifiers of current ST and PPs.

2562 FDP_RIP.1/EAC2PP
 2563 Subset residual information protection

2564 Hierarchical to: No other components

2565 Dependencies: No dependencies

2566 FDP_RIP.1.1_EAC2PP

2567 The TSF shall ensure that any previous information content of a resource is made
 2568 unavailable upon the deallocation of the resource from¹⁶¹ the following objects:

- 2569 1. Session keys (PACE-K_{MAC}, PACE-K_{Enc}), (CA2-K_{MAC}, CA2-K_{Enc}) (immediately after
 2570 closing related communication session),
- 2571 2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared
 2572 secret K),
- 2573 3. Secret Electronic Document Holder Authentication Data, e.g. PIN and/or PUK
 2574 (when their temporarily stored values are not used any more)¹⁶².
- 2575 4. none.¹⁶³

2576 **79. Application note (taken from [6], application note 30)**

2577 The functional family FDP_RIP possesses such a general character, that it is applicable not
 2578 only to user data (as assumed by the class FDP), but also to TSF-Data; in this respect it is
 2579 similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1/EAC2PP
 2580 requires a certain quality metric (*any previous information content of a resource is made*

¹⁵⁸ [assignment: access control SFP]

¹⁵⁹ [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

¹⁶⁰ [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

¹⁶¹ [selection: allocation of the resource to, deallocation of the resource from]

¹⁶² [assignment: list of objects]

¹⁶³ [assignment: list of objects]

2581 *unavailable*) for key destruction in addition to FCS_CKM.4/EAC2PP that merely requires to
 2582 ensure key destruction according to a method/standard.

2583 [Application note 80 \(from ST author\)](#)

2584 The above SFR is slightly refined from [20] in order not to confuse Chip Authentication 1 with
 2585 Chip Authentication 2.

2586 FDP_UCT.1/TRM_EAC2PP
 2587 Basic data exchange confidentiality – MRTD

2588 Hierarchical to: No other components

2589 Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1
 2590 Trusted path] fulfilled by FTP_ITC.1/PACE_EAC2PP

2591 [FDP_ACC.1 Subset access control, or FDP_IFC.1
 2592 Subset information flow control] fulfilled by
 2593 FDP_ACC.1/TRM_EAC2PP

2594 FDP_UCT.1.1/TRM_EAC2PP

2595 The TSF shall enforce the Access Control SFP¹⁶⁴ to be able to transmit and receive¹⁶⁵
 2596 user data in a manner protected from unauthorised disclosure.

2597 FDP_UIT.1/TRM_EAC2PP
 2598 TRM Data exchange integrity

2599 Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1
 2600 Trusted path] fulfilled by FTP_ITC.1/PACE_EAC2PP

2601 [FDP_ACC.1 Subset access control, or FDP_IFC.1
 2602 Subset information flow control] fulfilled by
 2603 FDP_ACC.1/TRM_EAC2PP

2604 FDP_UIT.1.1/TRM_EAC2PP

2605 The TSF shall enforce the Access Control SFP¹⁶⁶ to be able to transmit and receive¹⁶⁷
 2606 user data in a manner protected from modification, deletion, insertion and replay¹⁶⁸ errors.

¹⁶⁴ [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

¹⁶⁵ [selection: *transmit, receive*]

¹⁶⁶ [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

¹⁶⁷ [selection: *transmit, receive*]

¹⁶⁸ [selection: *modification, deletion, insertion, replay*]

2607 FDP UIT.1.2/TRM_EAC2PP

2608 The TSF shall be able to determine on receipt of user data, whether modification, deletion,
 2609 insertion and replay¹⁶⁹ has occurred.

2610 The following SFRs are imported due to claiming [5]. They concern access control mechanisms
 2611 related to EAC1-protected data.

2612 • **FDP_ACC.1/TRM_EAC1PP**

2613 The above is equivalent **FDP_ACC.1/TRM_EAC2PP**, since EF.SOD (cf. FDP_ACC.1/TRM in
 2614 [5]) can be considered user data.; cf. also the application note below FDP_ACF.1/TRM.

2615 • **FDP_ACF.1/TRM_EAC1PP**

2616 The above is covered by **FDP_ACF.1/TRM**; cf. Application Note there.

2617 • **FDP_RIP.1/EAC1PP**

2618 • **FDP_UCT.1/TRM_EAC1PP**

2619 (equivalent to **FDP_UCT.1/TRM_EAC2PP**, but listed here for the sake of completeness)

2620 • **FDP_UIT.1/TRM_EAC1PP**

2621 (equivalent to **FDP_UIT.1/TRM_EAC2PP**, but listed here for the sake of completeness)

2622 FDP_RIP.1/EAC1PP

2623 Subset residual information protection

2624 Hierarchical to: No other components

2625 Dependencies: No dependencies

2626 FDP_RIP.1.1/EAC1PP

2627 The TSF shall ensure that any previous information content of a resource is made
 2628 unavailable upon the deallocation of the resource from¹⁷⁰ the following objects:

2629 1. Session Keys (immediately after closing related communication session),

¹⁶⁹ [selection: *modification, deletion, insertion, replay*]

¹⁷⁰ [selection: *allocation of the resource to, deallocation of the resource from*]

- 2630 2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared
- 2631 secret K¹⁷¹).¹⁷²
- 2632 3. none.¹⁷³

2633 The following SFRs are imported due to claiming [14]. They concern access control
 2634 mechanisms of an eSign application.

- 2635 • **FDP_ACC.1/SCD/SVD_Generation_SSCDPP**
- 2636 • **FDP_ACF.1/SCD/SVD_Generation_SSCDPP**
- 2637 • **FDP_ACC.1/SVD_Transfer_SSCDPP**
- 2638 • **FDP_ACF.1/SVD_Transfer_SSCDPP**
- 2639 • **FDP_ACC.1/Signature-creation_SSCDPP**
- 2640 • **FDP_ACF.1/Signature-creation_SSCDPP**
- 2641 • **FDP_RIP.1/SSCDPP**
- 2642 • **FDP_SDI.2/Persistent_SSCDPP**
- 2643 • **FDP_SDI.2/DTBS_SSCDPP**

2644 FDP_ACC.1/SCD/SVD_Generation_SSCDPP

2645 Subset access control

2646 Hierarchical to: No other components

2647 Dependencies: FDP_ACF.1 Security attribute based access control
 2648 fulfilled by

2649 FDP_ACF.1/SCD/SVD_Generation_SSCDPP

2650 FDP_ACC.1.1/SCD/SVD_Generation_SSCDPP

2651 The TSF shall enforce the SCD/SVD Generation SFP¹⁷⁴ on

- 2652 1. subjects: S.User,
- 2653 2. objects: SCD, SVD,
- 2654 3. operations: generation of SCD/SVD pair.¹⁷⁵

2655 FDP_ACF.1/SCD/SVD_Generation_SSCDPP

2656 Security attribute based access control

¹⁷¹ according to [7]

¹⁷² [assignment: *list of objects*]

¹⁷³ [assignment: *list of objects*]

¹⁷⁴ [assignment: *access control SFP*]

¹⁷⁵ [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

- 2657 Hierarchical to: No other components
- 2658 Dependencies: FDP_ACC.1 Subset access control fulfilled by
2659 FDP_ACC.1/SCD/SVD_Generation_SSCDPP
- 2660 FMT_MSA.3 Static attribute initialisation fulfilled by
2661 FMT_MSA.3/SSCDPP
- 2662 FDP_ACF.1.1/SCD/SVD_Generation_SSCDPP
- 2663 The TSF shall enforce the SCD/SVD Generation SFP¹⁷⁶ to objects based on the following:
2664 the user S.User is associated with the security attribute “SCD/SVD Management”.¹⁷⁷
- 2665 FDP_ACF.1.2/SCD/SVD_Generation_SSCDPP
- 2666 The TSF shall enforce the following rules to determine if an operation among controlled
2667 subjects and controlled objects is allowed: S.User with the security attribute “SCD/SVD
2668 Management” set to “authorised” is allowed to generate SCD/SVD pair.¹⁷⁸
- 2669 FDP_ACF.1.3/SCD/SVD_Generation_SSCDPP
- 2670 The TSF shall explicitly authorise access of subjects to objects based on the following
2671 additional rules: none.¹⁷⁹
- 2672 FDP_ACF.1.4/SCD/SVD_Generation_SSCDPP
- 2673 The TSF shall explicitly deny access of subjects to objects based on the following
2674 additional rules: S.User with the security attribute “SCD/SVD management” set to “not
2675 authorised” is not allowed to generate SCD/SVD pair.¹⁸⁰
- 2676 FDP_ACC.1/SVD_Transfer_SSCDPP
2677 Subset access control
- 2678 Hierarchical to: No other components

¹⁷⁶ [assignment: *access control SFP*]

¹⁷⁷ [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

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

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

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

- 2679 Dependencies: FDP_ACF.1 Security attribute based access control
2680 fulfilled by FDP_ACF.1/SVD_Transfer_SSCDPP
- 2681 FDP_ACC.1.1/SVD_Transfer_SSCDPP
- 2682 The TSF shall enforce the SVD Transfer SFP¹⁸¹ on
- 2683 1. subjects: S.User,
 - 2684 2. objects: SVD
 - 2685 3. operations: export.¹⁸²
- 2686 FDP_ACF.1/SVD_Transfer_SSCDPP
2687 Security attribute based access control
- 2688 Hierarchical to: No other components
- 2689 Dependencies: FDP_ACC.1 Subset access control fulfilled by
2690 FDP_ACC.1/SVD_Transfer_SSCDPP
- 2691 FMT_MSA.3 Static attribute initialisation fulfilled by
2692 FMT_MSA.3/SSCDPP
- 2693 FDP_ACF.1.1/SVD_Transfer_SSCDPP
- 2694 The TSF shall enforce the SVD Transfer SFP¹⁸³ to objects based on the following:
- 2695 1. the S.User is associated with the security attribute Role,
 - 2696 2. the SVD.¹⁸⁴
- 2697 FDP_ACF.1.2/SVD_Transfer_SSCDPP
- 2698 The TSF shall enforce the following rules to determine if an operation among controlled
2699 subjects and controlled objects is allowed: R.Admin¹⁸⁵ is allowed to export SVD.¹⁸⁶
- 2700 FDP_ACF.1.3/SVD_Transfer_SSCDPP

¹⁸¹ [assignment: *access control SFP*]

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

¹⁸³ [assignment: *access control SFP*]

¹⁸⁴ [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

¹⁸⁵ [selection: *R.Admin, R.Sigy*]

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

- 2701 The TSF shall explicitly authorise access of subjects to objects based on the following
 2702 additional rules: none.¹⁸⁷
- 2703 FDP_ACF.1.4/SVD_Transfer_SSCDPP
- 2704 The TSF shall explicitly deny access of subjects to objects based on the following
 2705 additional rules: none.¹⁸⁸
- 2706 **81. Application note (taken from [14], application note 9)**
- 2707 Applied.
- 2708 FDP_ACC.1/Signature-creation_SSCDPP
 2709 Subset access control
- 2710 Hierarchical to: No other components
- 2711 Dependencies: FDP_ACF.1 Security attribute based access control
 2712 fulfilled by FDP_ACF.1/Signature-creation_SSCDPP
- 2713 FDP_ACC.1.1/Signature_Creation
- 2714 The TSF shall enforce the Signature Creation SFP¹⁸⁹ on
- 2715 1. subjects: S.User,
 2716 2. objects: DTBS/R, SCD,
 2717 3. operations: signature creation.¹⁹⁰
- 2718 FDP_ACF.1/Signature-creation_SSCDPP
 2719 Security attribute based access control
- 2720 Hierarchical to: No other components
- 2721 Dependencies: FDP_ACC.1 Subset access control fulfilled by
 2722 FDP_ACC.1/Signature-creation_SSCDPP
- 2723 FMT_MSA.3 Static attribute initialisation fulfilled by
 2724 FMT_MSA.3/SSCDPP
- 2725 FDP_ACF.1.1/Signature_Creation_SSCDPP

¹⁸⁷ [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

¹⁸⁸ [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

¹⁸⁹ [assignment: access control SFP]

¹⁹⁰ [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

- 2726 The TSF shall enforce the Signature Creation SFP¹⁹¹ to objects based on the following:
- 2727 1. the user S.User is associated with the security attribute “Role” and
- 2728 2. the SCD with the security attribute “SCD Operational”.¹⁹²
- 2729 FDP_ACF.1.2/Signature_Creation_SSCDPP
- 2730 The TSF shall enforce the following rules to determine if an operation among controlled
- 2731 subjects and controlled objects is allowed: R.Sigy is allowed to create electronic
- 2732 signatures for DTBS/R with SCD which security attribute “SCD operational” is set to
- 2733 “yes”.¹⁹³
- 2734 FDP_ACF.1.3/Signature_Creation_SSCDPP
- 2735 The TSF shall explicitly authorise access of subjects to objects based on the following
- 2736 additional rules: none.¹⁹⁴
- 2737 FDP_ACF.1.4/Signature_Creation_SSCDPP
- 2738 The TSF shall explicitly deny access of subjects to objects based on the following
- 2739 additional rules: S.User is not allowed to create electronic signatures for DTBS/R with SCD
- 2740 which security attribute “SCD operational” is set to “no”.¹⁹⁵
- 2741 FDP_RIP.1/SSCDPP
- 2742 Subset residual information protection
- 2743 Hierarchical to: No other components
- 2744 Dependencies: No dependencies
- 2745 FDP_RIP.1.1_SSCDPP
- 2746 The TSF shall ensure that any previous information content of a resource is made
- 2747 unavailable upon the de-allocation of the resource from¹⁹⁶ the following objects: SCD¹⁹⁷.

¹⁹¹ [assignment: access control SFP]

¹⁹² [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

¹⁹³ [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

¹⁹⁴ [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

¹⁹⁵ [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

¹⁹⁶ [selection: allocation of the resource to, deallocation of the resource from]

¹⁹⁷ [assignment: list of objects]

- 2748 FDP_SDI.2/Persistent_SSCDPP
- 2749 Stored data integrity monitoring and action
- 2750 Hierarchical to: FDP_SDI.1 Stored data integrity monitoring
- 2751 Dependencies: No dependencies
- 2752 FDP_SDI.2.1/Persistent_SSCDPP
- 2753 The TSF shall monitor user data stored in containers controlled by the TSF for integrity
- 2754 error¹⁹⁸ on all objects, based on the following attributes: integrity checked stored data¹⁹⁹.
- 2755 FDP_SDI.2.2/Persistent_SSCDPP
- 2756 Upon detection of a data integrity error, the TSF shall
- 2757 1. prohibit the use of the altered data
- 2758 2. inform the S.Sigy about integrity error.²⁰⁰
- 2759 **82. Application note (taken from [14])**
- 2760 The [14] was defined the followings:
- 2761 The following data persistently stored by the TOE shall have the user data attribute "integrity
- 2762 checked persistent stored data":
- 2763 1) SCD
- 2764 2) SVD (if persistently stored by the TOE).
- 2765 The DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked
- 2766 stored data"
- 2767 FDP_SDI.2/DTBS_SSCDPP
- 2768 Stored data integrity monitoring and action
- 2769 Hierarchical to: FDP_SDI.1 Stored data integrity monitoring
- 2770 Dependencies: No dependencies
- 2771 FDP_SDI.2.1/DTBS_SSCDPP

¹⁹⁸ [assignment: *integrity errors*]

¹⁹⁹ [assignment: *user data attributes*]

²⁰⁰ [assignment: *action to be taken*]

2772 The TSF shall monitor user data stored in containers controlled by the TSF for integrity
 2773 error²⁰¹ on all objects, based on the following attributes: integrity checked stored DTBS.²⁰²

2774 FDP_SDI.2.2/DTBS_SSCDPP

2775 Upon detection of a data integrity error, the TSF shall

- 2776 1. prohibit the use of the altered data
- 2777 2. inform the S.Siqy about integrity error.²⁰³

2778 **83. Application note (taken from [14], application note 10)**

2779 The integrity of TSF data like RAD shall be protected to ensure the effectiveness of the user
 2780 authentication. This protection is a specific aspect of the security architecture (cf.
 2781 ADV_ARC.1).

2782 **6.1.4. Class FTP**

2783 The following SFRs are imported from [6].

- 2784 • **FTP_ITC.1/PACE_EAC2PP**
- 2785 • **FTP_ITC.1/CA_EAC2PP**

2786 **FTP_ITC.1/PACE_EAC2PP**
 2787 **Inter-TSF trusted channel after PACE**

2788 Hierarchical to: No other components

2789 Dependencies: No dependencies

2790 **FTP_ITC.1.1/PACE_EAC2PP**

2791 The TSF shall provide a communication channel between itself and ~~another trusted IT~~
 2792 ~~product~~ a **PACE terminal** that is logically distinct from other communication channels and
 2793 provides assured identification of its end points and protection of the channel data from
 2794 modification or disclosure. **The trusted channel shall be established by performing the**
 2795 **PACE protocol according to [17].**

2796 **FTP_ITC.1.2/PACE_EAC2PP**

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

2797 The TSF shall permit ~~another trusted IT product~~ **a PACE terminal**²⁰⁴ to initiate
2798 communication via the trusted channel.

2799 FTP_ITC.1.3/PACE_EAC2PP

2800 The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data
2801 exchange between the TOE and a PACE terminal after PACE.²⁰⁵

2802 **84. Application note (taken from [6], application note 31)**

2803 The above definition refines FTP_ITC.1 from [13]. The definitions there are unclear as to what
2804 the “other trusted IT product” actually is. Since we distinguish here between trusted channels
2805 that are established once after PACE, and then then (re)established after CA2, the above
2806 refinement is necessary for clarification.

2807 FTP_ITC.1/CA_EAC2PP
2808 Inter-TSF trusted channel after CA2

2809 Hierarchical to: No other components

2810 Dependencies: No dependencies

2811 FTP_ITC.1.1/CA2_EAC2PP

2812 The TSF shall provide a communication channel between itself and ~~another trusted IT~~
2813 ~~product~~ **an EAC2 terminal** that is logically distinct from other communication channels
2814 and provides assured identification of its end points and protection of the channel data
2815 from modification or disclosure. **The trusted channel shall be established by**
2816 **performing the CA2 protocol according to [17].**

2817 FTP_ITC.1.2/CA2_EAC2PP

2818 The TSF shall permit ~~another trusted IT product~~ **an EAC2 terminal**²⁰⁶ to initiate
2819 communication via the trusted channel.

2820 FTP_ITC.1.3/CA2_EAC2PP

2821 The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data
2822 exchange between the TOE and an EAC2 terminal after Chip Authentication 2.²⁰⁷

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

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

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

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

2823 85. Application note (taken from [6], application note 32)

2824 The trusted channel is established after successful performing the PACE protocol
2825 (FIA_UAU.1/PACE_EAC2PP), the TA2 protocol (FIA_UAU.1/EAC2_Terminal_EAC2PP) and
2826 the CA2 protocol (FIA_API.1/CA_EAC2PP). If Chip Authentication 2 was successfully
2827 performed, secure messaging is immediately restarted using the derived session keys (CA-
2828 K_{MAC} , CA- K_{Enc})²⁰⁸. This secure messaging enforces the required properties of operational
2829 trusted channel; the cryptographic primitives being used for the secure messaging are as
2830 required by FCS_COP.1/PACE_ENC_EAC2PP and FCS_COP.1/PACE_MAC_EAC2PP.

2831 The following SFR is imported due to claiming [5]. It concerns applications with EAC1-
2832 protected data.

2833 • **FTP_ITC.1/PACE_EAC1PP**

2834 FTP_ITC.1/PACE_EAC1PP
2835 Inter-TSF trusted channel after PACE

2836 Hierarchical to: No other components

2837 Dependencies: No dependencies

2838 FTP_ITC.1.1/PACE_EAC1PP

2839 The TSF shall provide a communication channel between itself and another trusted IT
2840 product that is logically distinct from other communication channels and provides assured
2841 identification of its end points and protection of the channel data from modification or
2842 disclosure.

2843 FTP_ITC.1.2/PACE_EAC1PP

2844 The TSF shall permit another trusted IT product to initiate communication via the trusted
2845 channel.

2846 FTP_ITC.1.3/PACE_EAC1PP

2847 The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data
2848 exchange between the TOE and the Terminal.²⁰⁹

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

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

2849 **6.1.5. Class FAU**

2850 The following SFR is imported due to claiming [6]. It concerns applications with EAC2-
2851 protected data.

2852 • **FAU_SAS.1/EAC2PP**

2853 FAU_SAS.1/EAC2PP
2854 Audit storage

2855 Hierarchical to: No other components

2856 Dependencies: No dependencies

2857 FAU_SAS.1.1_EAC2PP

2858 The TSF shall provide the Manufacturer²¹⁰ with the capability to store the Initialisation and
2859 Pre-Personalisation Data²¹¹ in the audit records.

2860 The following SFR is imported due to claiming [5]. It concerns applications with EAC1-
2861 protected data.

2862 • **FAU_SAS.1/EAC1PP**

2863 (equivalent to **FAU_SAS.1/EAC2PP**, but listed here for the sake of completeness)

2864 **6.1.6. Class FMT**

2865 FMT_SMR.1
2866 Security roles

2867 Hierarchical to: No other components

2868 Dependencies: FIA_UID.1 Timing of identification: fulfilled by
2869 FIA_UID.1/PACE_EAC1PP,
2870 FIA_UID.1/PACE_EAC2PP,
2871 FIA_UID.1/EAC2_Terminal_EAC2PP

2872 FMT_SMR.1.1

²¹⁰ [assignment: *authorised users*]

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

2873 The TSF shall maintain the roles

- 2874 1. Manufacturer,
- 2875 2. Personalization Agent,
- 2876 3. Country Verifying Certification Authority (CVCA),
- 2877 4. Document Verifier (DV),
- 2878 5. Terminal,
- 2879 6. PACE Terminal,
- 2880 7. EAC2 terminal, if the eID, ePassport and/or eSign application are active,
- 2881 8. EAC1 terminal, if the ePassport application is active,
- 2882 9. Electronic Document Holder.²¹²

2883 FMT_SMR.1.2

2884 The TSF shall be able to associate users with roles.

2885 The next SFRs are imported from [6]. They concern mainly applications with EAC2-protected
2886 data.

- 2887 • **FMT_MTD.1/CVCA_INI_EAC2PP**
- 2888 • **FMT_MTD.1/CVCA_UPD_EAC2PP**
- 2889 • **FMT_SMF.1/EAC2PP**
- 2890 • **FMT_SMR.1/PACE_EAC2PP**

2891 This SFR is combined with FMT_SMR.1/PACE_EAC1PP into to by **FMT_SMR.1.**

- 2892 • **FMT_MTD.1/DATE_EAC2PP**
- 2893 • **FMT_MTD.1/PA_EAC2PP**
- 2894 • **FMT_MTD.1/SK_PICC_EAC2PP**
- 2895 • **FMT_MTD.1/KEY_READ_EAC2PP**
- 2896 • **FMT_MTD.1/Initialize_PIN_EAC2PP**
- 2897 • **FMT_MTD.1/Change_PIN_EAC2PP**
- 2898 • **FMT_MTD.1/Resume_PIN_EAC2PP**
- 2899 • **FMT_MTD.1/Unblock_PIN_EAC2PP**
- 2900 • **FMT_MTD.1/Activate_PIN_EAC2PP**
- 2901 • **FMT_MTD.3/EAC2PP**

²¹² [assignment: *the authorized identified roles*]

2902 • **FMT_LIM.1/EAC2PP**

2903 [86. Application note \(taken from \[20\], application note 12\)](#)

2904 The above SFR concerns the whole TOE, not just applications with EAC2-protected data.

2905 • **FMT_LIM.2/EAC2PP**

2906 [87. Application note \(taken from \[20\], application note 13\)](#)

2907 The above SFR concerns the whole TOE, not just applications with EAC2-protected data.

2908 • **FMT_MTD.1/INI_ENA_EAC2PP**

2909 • **FMT_MTD.1/INI_DIS_EAC2PP**

2910 FMT_MTD.1/CVCA_INI_EAC2PP

2911 Management of TSF data – Initialization of CVCA Certificate and Current Date

2912 Hierarchical to: No other components

2913 Dependencies: FMT_SMF.1 Specification of management functions:

2914 fulfilled by FMT_SMF.1/EAC2PP

2915 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/

2916 EAC2PP

2917 FMT_MTD.1.1/CVCA_INI_EAC2PP

2918 The TSF shall restrict the ability to write²¹³ the

2919 1. initial CVCA Public Key,

2920 2. meta-data of the initial CVCA Certificate as required in [17], resp. [18],

2921 3. initial Current Date,

2922 4. none²¹⁴

2923 to the Personalization Agent.²¹⁵²¹⁶

2924 [88. Application note \(taken from \[6\], application note 36\)](#)

²¹³ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²¹⁴ [assignment: *list of TSF data*]

²¹⁵ [assignment: *the authorized identified roles*]

²¹⁶ [selection: *the manufacturer, the personalization agent*]

2925 The initial CVCA Public Key may be written by the manufacturer in the manufacturing phase
 2926 or by the Personalization Agent in the issuing phase (cf. [17]). The initial CVCA Public Keys
 2927 and their updates later on are used to verify the CVCA Link-Certificates.

2928 FMT_MTD.1/CVCA_UPD_EAC2PP
 2929 Management of TSF data – Country Verifying Certification Authority

2930 Hierarchical to: No other components

2931 Dependencies: FMT_SMF.1 Specification of management functions:
 2932 fulfilled by FMT_SMF.1/EAC2PP

2933 FMT_SMR.1 Security roles: fulfilled by
 2934 FMT_SMR.1/PACE_EAC2PP

2935 FMT_MTD.1.1/CVCA_UPD_EAC2PP

2936 The TSF shall restrict the ability to update²¹⁷ the

- 2937 1. CVCA Public Key (PK_{CVCA}),
- 2938 2. meta-data of the CVCA Certificate as required by [17], resp. [18],²¹⁸
- 2939 3. none²¹⁹

2940 to the Country Verifying Certification Authority.²²⁰

2941 **89. Application note (taken from [6], application note 37)**

2942 The CVCA updates its asymmetric key pair and distributes the public key and related meta-
 2943 data by means of CVCA Link-Certificates. The TOE updates its internal trust-point, if a valid
 2944 CVCA Link-Certificate (cf. FMT_MTD.3/EAC2PP) is provided by the terminal (cf. [18]).

2945 FMT_SMF.1/EAC2PP
 2946 Specification of Management Functions

2947 Hierarchical to: No other components

2948 Dependencies: No dependencies

2949 FMT_SMF.1.1/EAC2PP

2950 The TSF shall be capable of performing the following management functions:

²¹⁷ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²¹⁸ [assignment: *list of TSF data*]

²¹⁹ [assignment: *list of TSF data*]

²²⁰ [assignment: *the authorized identified roles*]

- 2951 1. Initialization.
- 2952 2. Pre-Personalization.
- 2953 3. Personalization.
- 2954 4. Configuration.
- 2955 5. Resume and unblock the PIN (if any).
- 2956 6. Activate and deactivate the PIN (if any).²²¹

2957 90. Application note (taken from [6], application note 33)

2958 The capability of PIN management gives additional security to the TOE.

2959 91. Application note (taken from [6], application note 34)

2960 The SFR is here refined by including mechanisms for PIN management. A TOE without PIN
 2961 management functionality can only use a commonly shared secret (such as the MRZ – in the
 2962 case of an ID document – or the CAN) during execution of PACE to control access to sensitive
 2963 information. A PIN however must not be shared and thus can be kept secret by the user.
 2964 Hence, this refinement of FMT_SMF.1/EAC2PP increases protection of user data by allowing
 2965 PIN access, and thus does not violate strict conformity to [13].

2966 FMT_MTD.1/DATE_EAC2PP
 2967 Management of TSF data – Current date

2968 Hierarchical to: No other components

2969 Dependencies: FMT_SMF.1 Specification of management functions
 2970 fulfilled by FMT_SMF.1/EAC2PP

2971 FMT_SMR.1 Security roles fulfilled by
 2972 FMT_SMR.1/PACE_EAC2PP

2973 FMT_MTD.1.1/DATE_EAC2PP

2974 The TSF shall restrict the ability to modify²²² the current date²²³ to

- 2975 1. CVCA.
- 2976 2. Document Verifier.
- 2977 3. EAC2 terminal (Authentication Terminal and Signature Terminal²²⁴) possessing an
 2978 Accurate Terminal Certificate according to [18].²²⁵

²²¹ [assignment: list of management functions to be provided by the TSF]
²²² [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
²²³ [assignment: list of TSF data]
²²⁴ [assignment: list of EAC2 terminal types]
²²⁵ [assignment: the authorized identified roles]

- 2979 4. none²²⁶
- 2980 **92. Application note (taken from [6], application note 38)**
- 2981 The authorized roles are identified in their certificates (cf. [17]) and are authorized by validating
 2982 the certificate chain up to the CVCA (cf. FMT_MTD.3/EAC2PP). The authorized role of a
 2983 terminal is part of the Certificate Holder Authorization in the card verifiable certificate that is
 2984 provided by the terminal within Terminal Authentication 2 (cf. [18]). Different types of EAC2
 2985 terminals may exist, cf. [17].
- 2986 FMT_MTD.1/PA_EAC2PP
 2987 Management of TSF data – Personalization Agent
- 2988 Hierarchical to: No other components
- 2989 Dependencies: FMT_SMF.1 Specification of management functions
 2990 fulfilled by FMT_SMF.1/EAC2PP
- 2991 FMT_SMR.1 Security roles fulfilled by
 2992 FMT_SMR.1/PACE_EAC2PP
- 2993 FMT_MTD.1.1/PA_EAC2PP
- 2994 The TSF shall restrict the ability to write²²⁷ the **card/chip security object(s) (SO_C) and**
 2995 **the document Security Object (SO_D)**²²⁸ to the Personalization Agent²²⁹.
- 2996 **93. Application note (taken from [6], application note 39)**
- 2997 Note that the card/chip security objects are mentioned here as well. These contain information,
 2998 such as algorithm identifiers, only necessary for EAC2. All requirements formulated in [13] are
 2999 thus met, and strict conformance is therefore not violated
- 3000 FMT_MTD.1/SK_PICC_EAC2PP
 3001 Management of TSF data – Chip Authentication and Restricted Identification Private Key(s)
- 3002 Hierarchical to: No other components
- 3003 Dependencies: FMT_SMF.1 Specification of management functions
 3004 fulfilled by FMT_SMF.1/EAC2PP
- 3005 FMT_SMR.1 Security roles fulfilled by
 3006 FMT_SMR.1/PACE_EAC2PP

²²⁶ [assignment: *the authorized identified roles*]

²²⁷ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²²⁸ [assignment: *list of TSF data*]

²²⁹ [assignment: *the authorized identified roles*]

3007 FMT_MTD.1.1/SK_PICC_EAC2PP

3008 The TSF shall restrict the ability to create or load²³⁰²³¹ the Chip Authentication private
 3009 key(s) (SK_{PICC}) and the Restricted Identification Private Key(s)²³² to the Personalization
 3010 Agent or the Manufacturer.²³³

3011 94. Application note (taken from [6], application note 40)

3012 Applied, see FCS_CKM.1/CA2 and FCS_CKM.1/RI.

3013 95. Application note (from ST author)

3014 The **FMT_MTD.1/SK_PICC_EAC2PP** was refined, because the Manufacturer means here the
 3015 electronic document manufacturer, which may create the application and the file system as
 3016 well. So the Manufacturer may generate or load the private keys.

3017 FMT_MTD.1/KEY_READ_EAC2PP

3018 Management of TSF data – Private Key Read

3019 Hierarchical to: No other components

3020 Dependencies: FMT_SMF.1 Specification of management functions
 3021 fulfilled by FMT_SMF.1/EAC2PP

3022 FMT_SMR.1 Security roles fulfilled by
 3023 FMT_SMR.1/PACE_EAC2PP

3024 FMT_MTD.1.1/KEY_READ_EAC2PP

3025 The TSF shall restrict the ability to read²³⁴ the

- 3026 1. PACE passwords,
- 3027 2. Personalization Agent Keys,
- 3028 3. the Chip Authentication private key(s) (SK_{PICC})
- 3029 4. the Restricted Identification private key(s)²³⁵
- 3030 5. none²³⁶

²³⁰ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²³¹ [selection: *create, load*]

²³² [assignment: *list of TSF data*]

²³³ [assignment: *the authorized identified roles*]

²³⁴ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²³⁵ [assignment: *list of TSF data*]

²³⁶ [assignment: *list of TSF data*]

- 3031 to none²³⁷
- 3032 [96. Application note \(taken from \[6\], application note 41\)](#)
- 3033 FMT_MTD.1/KEY_READ_EAC2PP extends the SFR from [13] by additional assignments.
- 3034 FMT_MTD.1/Initialize_PIN_EAC2PP
- 3035 PIN Management of TSF data – Initialize PIN
- 3036 Hierarchical to: No other components
- 3037 Dependencies: FMT_SMF.1 Specification of management functions
- 3038 fulfilled by FMT_SMF.1/EAC2PP
- 3039 FMT_SMR.1 Security roles fulfilled by
- 3040 FMT_SMR.1/PACE_EAC2PP
- 3041 FMT_MTD.1.1/Initialize_PIN_EAC2PP
- 3042 The TSF shall restrict the ability to write²³⁸ the initial PIN and PUK²³⁹ to the Personalization
- 3043 Agent²⁴⁰
- 3044 FMT_MTD.1/Change_PIN_EAC2PP
- 3045 Management of TSF data – Changing PIN
- 3046 Hierarchical to: No other components
- 3047 Dependencies: FMT_SMF.1 Specification of management functions
- 3048 fulfilled by FMT_SMF.1/EAC2PP
- 3049 FMT_SMR.1 Security roles fulfilled by
- 3050 FMT_SMR.1/PACE_EAC2PP
- 3051 FMT_MTD.1.1/Change_PIN_EAC2PP
- 3052 The TSF shall restrict the ability to change²⁴¹ the blocked PIN²⁴² to
- 3053 1. Electronic Document Holder (using the PUK) with unauthenticated terminal

²³⁷ [assignment: *the authorized identified roles*]

²³⁸ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²³⁹ [assignment: *list of TSF data*]

²⁴⁰ [assignment: *the authorized identified roles*]

²⁴¹ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²⁴² [assignment: *list of TSF data*]

- 3054 2. Authentication Terminal with the Terminal Authorisation level for PIN management
- 3055 according to [17]²⁴³²⁴⁴
- 3056 FMT_MTD.1/Resume_PIN_EAC2PP
- 3057 Management of TSF data – Resuming PIN
- 3058 Hierarchical to: No other components
- 3059 Dependencies: FMT_SMF.1 Specification of management functions
- 3060 fulfilled by FMT_SMF.1/EAC2PP
- 3061 FMT_SMR.1 Security roles fulfilled by
- 3062 FMT_SMR.1/PACE_EAC2PP
- 3063 FMT_MTD.1.1/Resume_PIN_EAC2PP
- 3064 The TSF shall restrict the ability to resume²⁴⁵ the suspended PIN²⁴⁶ to the Electronic
- 3065 Document Holder²⁴⁷
- 3066 **97. Application note (taken from [6], application note 42)**
- 3067 Resuming is a two-step procedure, subsequently using PACE with the CAN and PACE with
- 3068 the PIN. It must be implemented according to [17], and is relevant for the status as required by
- 3069 FIA_AFL.1/Suspend_PIN_EAC2PP. The Electronic Document Holder is authenticated as
- 3070 required by FIA_UAU.1/PACE_EAC2PP using the PIN as the shared password.
- 3071 FMT_MTD.1/Unblock_PIN_EAC2PP
- 3072 Management of TSF data – Unblocking PIN
- 3073 Hierarchical to: No other components
- 3074 Dependencies: FMT_SMF.1 Specification of management functions
- 3075 fulfilled by FMT_SMF.1/EAC2PP
- 3076 FMT_SMR.1 Security roles fulfilled by
- 3077 FMT_SMR.1/PACE_EAC2PP
- 3078 FMT_MTD.1.1/Unblock_PIN_EAC2PP

²⁴³ [assignment: *the authorized identified roles*]

²⁴⁴ [assignment: *the authorised identified roles that match the list of PIN changing rules conformant to [17]*]

²⁴⁵ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²⁴⁶ [assignment: *list of TSF data*]

²⁴⁷ [assignment: *the authorized identified roles*]

3079 The TSF shall restrict the ability to unblock²⁴⁸ the blocked PIN²⁴⁹ to

3080 1. the Electronic Document Holder (using the PUK for unblocking),

3081 2. an EAC2 terminal of a type that has the terminal authorization level for PIN

3082 management.²⁵⁰

3083 **98. Application note (taken from [6], application note 43)**

3084 The unblocking procedure must be implemented according to [17], and is relevant for the status

3085 as required by FIA_AFL.1/Block_PIN_EAC2PP. It can be triggered by either (i) the Electronic

3086 Document Holder being authenticated as required by FIA_UAU.1/PACE_EAC2PP using the

3087 PUK as the shared password or (ii) an EAC2 terminal (FIA_UAU.1/EAC2_Terminal_EAC2PP)

3088 that proved a terminal authorization level being sufficient for PIN management

3089 (FDP_ACF.1/TRM).

3090 FMT_MTD.1/Activate_PIN_EAC2PP

3091 Management of TSF data – Activating/Deactivating PIN

3092 Hierarchical to: No other components

3093 Dependencies: FMT_SMF.1 Specification of management functions

3094 fulfilled by FMT_SMF.1/EAC2PP

3095 FMT_SMR.1 Security roles fulfilled by

3096 FMT_SMR.1/PACE_EAC2PP

3097 FMT_MTD.1.1/Activate_PIN_EAC2PP

3098 The TSF shall restrict the ability to activate and deactivate²⁵¹ the PIN²⁵² to an EAC2

3099 terminal of a type that has the terminal authorization level for PIN management²⁵³.

3100 **99. Application note (taken from [6], application note 44)**

3101 The activation/deactivation procedures must be implemented according to [17]. They can be

3102 triggered by an EAC2 terminal (FIA_UAU.1/EAC2_Terminal_EAC2PP) that proved a terminal

3103 authorization level sufficient for PIN management (FDP_ACF.1/TRM).

3104 FMT_MTD.3/EAC2PP

3105 Secure TSF data

3106 Hierarchical to: No other components

²⁴⁸ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²⁴⁹ [assignment: *list of TSF data*]

²⁵⁰ [assignment: *the authorized identified roles*]

²⁵¹ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²⁵² [assignment: *list of TSF data*]

²⁵³ [assignment: *the authorized identified roles*]

3107 Dependencies: FMT_MTD.1 Management of TSF data fulfilled by
 3108 FMT_MTD.1/CVCA_INI_EAC2PP,
 3109 FMT_MTD.1/CVCA_UPD_EAC2PP,
 3110 FMT_MTD.1/DATE_EAC2PP

3111 FMT_MTD.3.1_EAC2PP

3112 The TSF shall ensure that only secure values **of the certificate chain** are accepted for
 3113 TSF data of the Terminal Authentication protocol 2 and the Access Control SFP²⁵⁴.

3114 **Refinement: To determine if the certificate chain is valid, the TOE shall proceed the**
 3115 **certificate validation according to [18].**

3116 **100. Application note (taken from [6], application note 45)**

3117 Terminal Authentication is used as required by (i) FIA_UID.1/EAC2_Terminal_EAC2PP and
 3118 FIA_UAU.5/PACE_EAC2PP. The terminal authorization level derived from the CVCA
 3119 Certificate, the DV Certificate and the Terminal Certificate is used as TSF-data for the access
 3120 control required by FDP_ACF.1/TRM.

3121 In addition, this ST contains all remaining SFRs of the claimed [13].

3122 FMT_LIM.1/EAC2PP
 3123 Limited capabilities

3124 Hierarchical to: No other components

3125 Dependencies: FMT_LIM.2 Limited availability: fulfilled by
 3126 FMT_LIM.2/EAC2PP

3127 FMT_LIM.1.1_EAC2PP

3128 The TSF shall be designed in a manner that limits their capabilities so that in conjunction
 3129 with 'Limited availability (FMT_LIM.2)' the following policy is enforced:

3130 Deploying test features after TOE delivery do not allow

- 3131 1. User Data to be manipulated and disclosed,
- 3132 2. TSF data to be manipulated or disclosed,
- 3133 3. software to be reconstructed,
- 3134 4. substantial information about construction of TSF to be gathered which may enable
 3135 other attacks.²⁵⁵ and

²⁵⁴ [assignment: *list of TSF data*]

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

- 3136 5. EAC1 and EAC2 protected data²⁵⁶
- 3137 **Application note 101 (from ST author)**
- 3138 The assignment was necessary to cover all protected user data.
- 3139 FMT_LIM.2/EAC2PP
- 3140 Limited availability
- 3141 Hierarchical to: No other components
- 3142 Dependencies: FMT_LIM.1 Limited capabilities: fulfilled by
- 3143 FMT_LIM.1/EAC2PP
- 3144 FMT_LIM.2.1_EAC2PP
- 3145 The TSF shall be designed in a manner that limits their availability so that in conjunction
- 3146 with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced:
- 3147 Deploying test features after TOE delivery do not allow
- 3148 1. User Data to be manipulated and disclosed.
- 3149 2. TSF data to be manipulated or disclosed.
- 3150 3. software to be reconstructed.
- 3151 4. substantial information about construction of TSF to be gathered which may enable
- 3152 other attacks.²⁵⁷ and
- 3153 5. EAC1 and EAC2 protected data²⁵⁸
- 3154 **Application note 102 (from ST author)**
- 3155 The assignment was necessary to cover all protected user data.
- 3156 FMT_MTD.1/INI_ENA_EAC2PP
- 3157 Management of TSF data – Writing Initialisation and Pre-personalisation Data
- 3158 Hierarchical to: No other components
- 3159 Dependencies: FMT_SMF.1 Specification of management functions:
- 3160 fulfilled by FMT_SMF.1/EAC2PP

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

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

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

- 3161 FMT_SMR.1 Security roles: fulfilled by
 3162 FMT_SMR.1/PACE_EAC2PP
- 3163 FMT_MTD.1.1/INI_ENA_EAC2PP
- 3164 The TSF shall restrict the ability to write²⁵⁹ the Initialisation Data and Pre-personalisation
 3165 Data²⁶⁰ to the Manufacturer.²⁶¹
- 3166 FMT_MTD.1/INI_DIS_EAC2PP
 3167 Management of TSF data – Reading and Using Initialisation and Pre-personalisation Data
- 3168 Hierarchical to: No other components
- 3169 Dependencies: FMT_SMF.1 Specification of management functions:
 3170 fulfilled by FMT_SMF.1/EAC2PP
- 3171 FMT_SMR.1 Security roles: fulfilled by
 3172 FMT_SMR.1/PACE_EAC2PP
- 3173 FMT_MTD.1.1/INI_DIS_EAC2PP
- 3174 The TSF shall restrict the ability to read out²⁶² the Initialisation Data and the Pre-
 3175 personalisation Data²⁶³ to the Personalisation Agent.²⁶⁴
- 3176 The following SFRs are imported due to claiming [5]. They mainly concern applications with
 3177 EAC1-protected data.
- 3178 • **FMT_SMF.1/EAC1PP**
 - 3179 • **FMT_SMR.1/PACE_EAC1PP**
- 3180 This SFR is combined with FMT_SMR.1/PACE_EAC2PP into **FMT_SMR.1**.
- 3181 • **FMT_LIM.1/EAC1PP**
- 3182 This SFR is equivalent to **FMT_LIM.1/EAC2PP**, but listed here for the sake of completeness.

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

²⁶⁰ [assignment: *list of TSF data*]

²⁶¹ [assignment: *the authorised identified roles*]

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

²⁶³ [assignment: *list of TSF data*]

²⁶⁴ [assignment: *the authorized identified roles*]

3183 • **FMT_LIM.2/EAC1PP**

3184 This SFR is equivalent to **FMT_LIM.2/EAC2PP**, but listed here for the sake of completeness.

3185 • **FMT_MTD.1/INI_ENA_EAC1PP**

3186 (equivalent to **FMT_MTD.1/INI_ENA_EAC2PP**, but listed here for the sake of completeness)

3187 • **FMT_MTD.1/INI_DIS_EAC1PP**

3188 (equivalent to **FMT_MTD.1/INI_DIS_EAC2PP**, but listed here for the sake of completeness)

3189 • **FMT_MTD.1/CVCA_INI_EAC1PP**

3190 • **FMT_MTD.1/CVCA_UPD_EAC1PP**

3191 • **FMT_MTD.1/DATE_EAC1PP**

3192 This SFR is equivalent to **FMT_MTD.1/DATE_EAC2PP**. Note that
 3193 **FMT_MTD.1/DATE_EAC2PP** generalizes the notion of Domestic Extended Inspection System
 3194 to EAC1 terminals with appropriate authorization level. This does not violate strict conformance
 3195 to [5].

3196 • **FMT_MTD.1/CAPK_EAC1PP**

3197 • **FMT_MTD.1/PA_EAC1PP**

3198 • **FMT_MTD.1/KEY_READ_EAC1PP**

3199 • **FMT_MTD.3/EAC1PP**

3200 **FMT_SMF.1/EAC1PP**

3201 Specification of Management Functions

3202 Hierarchical to: No other components

3203 Dependencies: No dependencies

3204 **FMT_SMF.1.1/EAC1PP**

3205 The TSF shall be capable of performing the following management functions:

3206 1. Initialization.

3207 2. Pre-personalisation.

3208 3. Personalisation

- 3209 4. Configuration.²⁶⁵
- 3210 FMT_MTD.1/CVCA_INI_EAC1PP
 3211 Management of TSF data – Initialization of CVCA Certificate and Current Date
- 3212 Hierarchical to: No other components
- 3213 Dependencies: FMT_SMF.1 Specification of management functions
 3214 fulfilled by FMT_SMF.1/EAC1PP
- 3215 FMT_SMR.1 Security roles fulfilled by
 3216 FMT_SMR.1/PACE_EAC1PP
- 3217 FMT_MTD.1.1/CVCA_INI_EAC1PP
- 3218 The TSF shall restrict the ability to write²⁶⁶ the
- 3219 1. initial Country Verifying Certification Authority Public Key,
 3220 2. initial Country Verifying Certification Authority Certificate,
 3221 3. initial Current Date,
 3222 4. none^{267,268}
- 3223 to Personalisation Agent²⁶⁹.
- 3224 **103. Application note (taken from [5], application note 41)**
- 3225 Applied.
- 3226 FMT_MTD.1/CVCA_UPD_EAC1PP
 3227 Management of TSF data – Country Verifying Certification Authority
- 3228 Hierarchical to: No other components
- 3229 Dependencies: FMT_SMF.1 Specification of management functions
 3230 functions fulfilled by FMT_SMF.1/EAC1PP
- 3231 FMT_SMR.1 Security roles fulfilled by
 3232 FMT_SMR.1/PACE_EAC1PP

²⁶⁵ [assignment: *list of management functions to be provided by the TSF*]

²⁶⁶ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²⁶⁷ [assignment: *list of TSF data*]

²⁶⁸ [assignment: *list of TSF data*]

²⁶⁹ [assignment: *the authorised identified roles*]

3233 FMT_MTD.1.1/CVCA_UPD_EAC1PP

3234 The TSF shall restrict the ability to update²⁷⁰ the

3235 1. Country Verifying Certification Authority Public Key,

3236 2. Country Verifying Certification Authority Certificate²⁷¹

3237 to Country Verifying Certification Authority.²⁷²

3238 **104. Application note (taken from [5], application note 42)**

3239 The Country Verifying Certification Authority updates its asymmetric key pair and distributes
 3240 the public key by means of the Country Verifying CA Link-Certificates (cf. [16]). The TOE
 3241 updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf.
 3242 FMT_MTD.3/EAC1PP) is provided by the terminal (cf. [16])

3243 FMT_MTD.1/CAPK_EAC1PP

3244 Management of TSF data – Chip Authentication Private Key

3245 Hierarchical to: No other components

3246 Dependencies: FMT_SMF.1 Specification of management functions
 3247 functions fulfilled by FMT_SMF.1/EAC1PP

3248 FMT_SMR.1 Security roles fulfilled by
 3249 FMT_SMR.1/PACE_EAC1PP

3250 FMT_MTD.1.1/CAPK_EAC1PP

3251 The TSF shall restrict the ability to create, load²⁷³²⁷⁴ the Chip Authentication Private Key²⁷⁵
 3252 to Manufacturer or Personalisation Agent.²⁷⁶

3253 **105. Application note (taken from [5], application note 44)**

3254 Applied.

3255 FMT_MTD.1/PA_EAC1PP

3256 Management of TSF data – Personalisation Agent

²⁷⁰ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²⁷¹ [assignment: *list of TSF data*]

²⁷² [assignment: *the authorised identified roles*]

²⁷³ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²⁷⁴ [selection: *create, load*]

²⁷⁵ [assignment: *list of TSF data*]

²⁷⁶ [assignment: *the authorised identified roles*]

3257	Hierarchical to:	No other components
3258	Dependencies:	FMT_SMF.1 Specification of management functions:
3259		fulfilled by FMT_SMF.1/EAC1PP
3260		FMT_SMR.1 Security roles: fulfilled by
3261		FMT_SMR.1/PACE_EAC1PP
3262	FMT_MTD.1.1/PA_EAC1PP	
3263	The TSF shall restrict the ability to <u>write</u> ²⁷⁷ the <u>Document Security Object (SO_D)</u> ²⁷⁸ to the	
3264	<u>Personalisation Agent</u> . ²⁷⁹	
3265	FMT_MTD.1/KEY_READ_EAC1PP	
3266	Management of TSF data – Key Read	
3267	Hierarchical to:	No other components
3268	Dependencies:	FMT_SMF.1 Specification of management functions:
3269		fulfilled by FMT_SMF.1/EAC1PP
3270		FMT_SMR.1 Security roles fulfilled by
3271		FMT_SMR.1/PACE_EAC1PP
3272		FMT_MTD.1.1/KEY_READ_EAC1PP
3273	The TSF shall restrict the ability to <u>read</u> ²⁸⁰ the	
3274	1. <u>PACE passwords</u> ,	
3275	2. <u>Chip Authentication Private Key</u> ,	
3276	3. <u>Personalisation Agent Keys</u> ²⁸¹	
3277	4. Active Authentication Private Key	
3278	to <u>none</u> ²⁸²	
3279	106. Application note (taken from [5], application note 45)	

²⁷⁷ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²⁷⁸ [assignment: *list of TSF data*]

²⁷⁹ [assignment: *the authorised identified roles*]

²⁸⁰ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

²⁸¹ [assignment: *list of TSF data*]

²⁸² [assignment: *the authorised identified roles*]

3280 The SFR FMT_MTD.1/KEY_READ_EAC1PP in the ST covers the definition in [13] and
 3281 extends it by additional TSF data. This extension does not conflict with the strict conformance
 3282 to [13].

3283 [107. Application note \(ST author\)](#)

3284 The refinement was necessary because of the Active Authentication protocol.

3285 FMT_MTD.3/EAC1PP

3286 Secure TSF data

3287 Hierarchical to: No other components

3288 Dependencies: FMT_MTD.1 Management of TSF data fulfilled by

3289 FMT_MTD.1/CVCA_INI_EAC1PP and

3290 FMT_MTD.1/CVCA_UPD_EAC1PP

3291 FMT_MTD.3.1_EAC1PP

3292 The TSF shall ensure that only secure values **of the certificate chain** are accepted for
 3293 TSF data of the Terminal Authentication Protocol v.1 and the Access Control.²⁸³

3294 **Refinement: The certificate chain is valid if and only if**

- 3295 **1. the digital signature of the Inspection System Certificate can be verified as**
 3296 **correct with the public key of the Document Verifier Certificate and the**
 3297 **expiration date of the Inspection System Certificate is not before the Current**
 3298 **Date of the TOE,**
- 3299 **2. the digital signature of the Document Verifier Certificate can be verified as**
 3300 **correct with the public key in the Certificate of the Country Verifying**
 3301 **Certification Authority and the expiration date of the Certificate of the Country**
 3302 **Verifying Certification Authority is not before the Current Date of the TOE and**
 3303 **the expiration date of the Document Verifier Certificate is not before the Current**
 3304 **Date of the TOE,**
- 3305 **3. the digital signature of the Certificate of the Country Verifying Certification**
 3306 **Authority can be verified as correct with the public key of the Country Verifying**
 3307 **Certification Authority known to the TOE.**

²⁸³ [assignment: *list of TSF data*]

3308 **The Inspection System Public Key contained in the Inspection System Certificate in**
 3309 **a valid certificate chain is a secure value for the authentication reference data of the**
 3310 **Extended Inspection System** EAC1 terminal.

3311 **The intersection of the Certificate Holder Authorizations contained in the**
 3312 **certificates of a valid certificate chain is a secure value for Terminal Authorization**
 3313 **of a successful authenticated Extended Inspection System** EAC1 terminal.

3314 [108. Application note \(taken from \[5\], application note 46\)](#)

3315 The Terminal Authentication Version 1 is used for EAC1 terminal as required by
 3316 FIA_UAU.4/PACE_EAC1PP and FIA_UAU.5/PACE_EAC1PP. The Terminal Authorization is
 3317 used as TSF data for access control required by FDP_ACF.1/TRM.

3318 The following SFRs are imported due to claiming [14]. They mostly concern the security
 3319 management of an *eSign* application.

- 3320 • **FMT_SMR.1/SSCDPP**
- 3321 • **FMT_SMF.1/SSCDPP**
- 3322 • **FMT_MOF.1/SSCDPP**
- 3323 • **FMT_MSA.1/Admin_SSCDPP**
- 3324 • **FMT_MSA.1/SignatorySSCDPP**
- 3325 • **FMT_MSA.2/SSCDPP**
- 3326 • **FMT_MSA.3/SSCDPP**
- 3327 • **FMT_MSA.4/SSCDPP**
- 3328 • **FMT_MTD.1/Admin_SSCDPP**
- 3329 • **FMT_MTD.1/Signatory_SSCDPP**

3330 FMT_SMR.1/SSCDPP
 3331 Security roles

3332 Hierarchical to: No other components

3333 Dependencies: FIA_UID.1 Timing of identification fulfilled by
 3334 FIA_UID.1/SSCDPP

3335 FMT_SMR.1.1/SSCDPP

3336 The TSF shall maintain the roles R.Admin and R.Sigy²⁸⁴

²⁸⁴ [assignment: *the authorised identified roles*]

3337 FMT_SMR.1.2/SSCDPP

3338 The TSF shall be able to associate users with roles.

3339 FMT_SMF.1/SSCDPP

3340 Security Management Functions

3341 Hierarchical to: No other components

3342 Dependencies: No dependencies

3343 FMT_SMF.1.1/SSCDPP

3344 The TSF shall be capable of performing the following management functions:

- 3345 1. Creation and modification of RAD,
- 3346 2. Enabling the signature creation function,
- 3347 3. Modification of the security attribute SCD/SVD management, SCD operational,
- 3348 4. Change the default value of the security attribute SCD Identifier,²⁸⁵
- 3349 5. Unblock the RAD²⁸⁶

3350 [109. Application note \(taken from \[14\], application note 14\)](#)

3351 Applied.

3352 FMT_MOF.1/SSCDPP

3353 Management of security functions behaviour

3354 Hierarchical to: No other components

3355 Dependencies: FMT_SMR.1 Security roles fulfilled by
3356 FMT_SMR.1/SSCDPP

3357 FMT_SMF.1 Specification of Management Functions
3358 fulfilled by FMT_SMF.1/SSCDPP

3359 FMT_MOF.1.1/SSCDPP

3360 The TSF shall restrict the ability to enable²⁸⁷ the functions signature creation function²⁸⁸ to
3361 R.Sigy²⁸⁹.

²⁸⁵ [assignment: list of other security management functions to be provided by the TSF]

²⁸⁶ [assignment: list of other security management functions to be provided by the TSF]

²⁸⁷ [selection: determine the behaviour of, disable, enable, modify the behaviour of]

²⁸⁸ [assignment: list of functions]

²⁸⁹ [assignment: the authorised identified roles]

- 3362 FMT_MSA.1/Admin_SSCDPP
 3363 Management Security attributes
- 3364 Hierarchical to: No other components
- 3365 Dependencies: [FDP_ACC.1 Subset access control or
 3366 FDP.IFC.1 Subset information flow control] fulfilled by
 3367 FDP_ACC.1/SCD/SVD_Generation_SSCDPP
- 3368 FMT_SMR.1 Security roles fulfilled by
 3369 FMT_SMR.1/SSCDPP
- 3370 FMT_SMF.1 Specification of Management Functions
 3371 fulfilled by FMT_SMF.1/SSCDPP
- 3372 FMT_MSA.1.1/Admin_SSCDPP
- 3373 The TSF shall enforce the SCD/SVD Generation SFP²⁹⁰ to restrict the ability to modify,
 3374 none²⁹¹ the security attributes SCD/SVD management²⁹² to R.Admin²⁹³.
- 3375 FMT_MSA.1/SignatorySSCDPP
 3376 Management Security attributes
- 3377 Hierarchical to: No other components
- 3378 Dependencies: [FDP_ACC.1 Subset access control or
 3379 FDP.IFC.1 Subset information flow control] fulfilled by
 3380 FDP_ACC.1/Signature-creation_SSCDPP
- 3381 FMT_SMR.1 Security roles fulfilled by
 3382 FMT_SMR.1/SSCDPP
- 3383 FMT_SMF.1 Specification of Management Functions
 3384 fulfilled by FMT_SMF.1/SSCDPP
- 3385 FMT_MSA.1.1/Signatory_SSCDPP

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

²⁹¹ [assignment: *other operations*]

²⁹² [assignment: *list of security attributes*]

²⁹³ [assignment: *the authorized identified roles*]

3386 The TSF shall enforce the SCD/SVD Generation SFP²⁹⁴ to restrict the ability to modify²⁹⁵
 3387 the security attributes SCD operational²⁹⁶ to R.Sigy²⁹⁷.

3388 FMT_MSA.2/SSCDPP
 3389 Secure security attributes

3390 Hierarchical to: No other components

3391 Dependencies: [FDP_ACC.1 Subset access control or
 3392 FDP.IFC.1 Subset information flow control] fulfilled by
 3393 FDP_ACC.1/SCD/SVD_Generation_SSCDPP and
 3394 FDP_ACC.1/Signature-creation_SSCDPP

3395 FMT_MSA.1 Management of security attributes fulfilled
 3396 by FMT_MSA.1/Admin_SSCDPP and
 3397 FMT_MSA.1/SignatorySSCDPP.

3398 FMT_SMR.1 Security roles fulfilled by
 3399 FMT_SMR.1/SSCDPP

3400 FMT_MSA.2.1/SSCDPP

3401 The TSF shall ensure that only secure values are accepted for SCD/SVD Management
 3402 and SCD operational²⁹⁸.

3403 **110. Application note (taken from [14], application note 15)**

3404 Applied.

3405 FMT_MSA.3/SSCDPP
 3406 Static attribute initialisation

3407 Hierarchical to: No other components

3408 Dependencies: FMT_MSA.1 Management of security attributes fulfilled
 3409 by FMT_MSA.1/Admin_SSCDPP and
 3410 FMT_MSA.1/SignatorySSCDPP.

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

3411 FMT_SMR.1 Security roles fulfilled by
 3412 FMT_SMR.1/SSCDPP

3413 FMT_MSA.3.1/ SSCDPP

3414 The TSF shall enforce the SCD/SVD Generation SFP, SVD Transfer SFP and Signature
 3415 Creation SFP²⁹⁹ to provide restrictive³⁰⁰ default values for security attributes that are used
 3416 to enforce SFP.

3417 FMT_MSA.3.2/ SSCDPP

3418 The TSF shall allow the R.Admin³⁰¹ to specify alternative initial values to override the
 3419 default values when an object or information created.

3420 FMT_MSA.4/SSCDPP
 3421 Security attribute value inheritance

3422 Hierarchical to: No other components

3423 Dependencies: [FDP_ACC.1 Subset access control or
 3424 FDP.IFC.1 Subset information flow control] fulfilled by
 3425 FDP_ACC.1/SCD/SVD_Generation_SSCDPP and
 3426 FDP_ACC.1/Signature-creation_SSCDPP

3427 FMT_MSA.4/SSCDPP

3428 The TSF shall use the following rules to set the value of security attributes:

- 3429 1. If S.Admin successfully generates an SCD/SVD pair without S.Sigy being
 3430 authenticated the security attribute “SCD operational of the SCD” shall be set to
 3431 “no” as a single operation.
- 3432 2. If S.Sigy successfully generates an SCD/SVD pair the security attribute “SCD
 3433 operational of the SCD” shall be set to “yes” as a single operation.³⁰²

3434 **111. Application note (taken from [14], application note 16)**

3435 The TOE may not support generating an SVD/SCD pair by the signatory alone, in which case
 3436 rule (2) is not relevant.

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

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

³⁰¹ [assignment: *the authorised identified roles*]

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

- 3437 FMT_MTD.1/Admin_SSCDPP
- 3438 Management of TSF data

- 3439 Hierarchical to: No other components

- 3440 Dependencies: FMT_SMR.1 Security roles fulfilled by
- 3441 FMT_SMR.1/SSCDPP

- 3442 FMT_SMF.1 Specification of Management Functions
- 3443 fulfilled by FMT_SMF.1/SSCDPP

- 3444 FMT_MTD.1.1/Admin_SSCDPP
- 3445 The TSF shall restrict the ability to create³⁰³ the RAD³⁰⁴ to R.Admin³⁰⁵.

- 3446 FMT_MTD.1/Signatory_SSCDPP
- 3447 Management of TSF data

- 3448 Hierarchical to: No other components

- 3449 Dependencies: FMT_SMR.1 Security roles fulfilled by
- 3450 FMT_SMR.1/SSCDPP

- 3451 FMT_SMF.1 Specification of Management Functions
- 3452 fulfilled by FMT_SMF.1/SSCDPP

- 3453 FMT_MTD.1.1/Signatory_SSCDPP
- 3454 The TSF shall restrict the ability to modify³⁰⁶, none³⁰⁷ the RAD³⁰⁸ to R.Sigy³⁰⁹.

- 3455 **112. Application note (taken from [14], application note 17)**
- 3456 Applied.
- 3457 The following SFRs are defined here. The concern loading applications onto the IC during
- 3458 manufacturing and relate directly to OT.Cap_Avail_Loader.

- 3459 FMT_LIM.1/Loader
- 3460 Limited Capabilities

³⁰³ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

³⁰⁴ [assignment: *list of TSF data*]

³⁰⁵ [assignment: *the authorised identified roles*]

³⁰⁶ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

³⁰⁷ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

³⁰⁸ [assignment: *list of TSF data*]

³⁰⁹ [assignment: *the authorised identified roles*]

- 3461 Hierarchical to: No other components
- 3462 Dependencies: FMT_ LIM.2 Limited availability fulfilled by
 3463 FMT_LIM.2/Loader
- 3464 FMT_LIM.1.1/Loader
- 3465 The TSF shall be designed and implemented in a manner that limits their capabilities so
 3466 that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced:
 3467 Deploying Loader functionality after the locking of the Loader³¹⁰ does not allow stored user
 3468 data to be disclosed or manipulated by unauthorized users.³¹¹
- 3469 **113. Application note (taken from [20], application note 14)**
- 3470 FMT_LIM.1/Loader supplements FMT_LIM.2/Loader allowing for non-overlapping loading of
 3471 user data and protecting the TSF against misuses of the Loader for attacks against the TSF.
 3472 The TOE Loader may allow for correction of already loaded user data before the assigned
 3473 action e.g. before blocking the TOE Loader for TOE Delivery to the end-customer or any
 3474 intermediate step on the life cycle of the Security IC or the smartcard.
- 3475 FMT_LIM.2/Loader
 3476 Limited Availability
- 3477 Hierarchical to: No other components
- 3478 Dependencies: FMT_ LIM.1 Limited capabilities fulfilled by
 3479 FMT_LIM.1/Loader
- 3480 FMT_LIM.2.1/Loader
- 3481 The TSF shall be designed and implemented in a manner that limits their availability so
 3482 that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced:
 3483 The TSF prevents deploying the Loader functionality after the locking of the Loader³¹²³¹³
- 3484 **114. Application note (taken from [20], application note 15)**
- 3485 The Loader functionality relies on a secure boot loading procedure in a secure environment
 3486 before TOE delivery to the assigned user and preventing to deploy the Loader of the Security
 3487 IC after an assigned action, e.g. after blocking the Loader for TOE delivery to the end-user.
- 3488 The following SFR is new and concern security management for ePassport application in
 3489 combination with [5] in case the Active Authentication protocol is active:

³¹⁰ [assignment: *action*]

³¹¹ [assignment: *Limited capability and availability policy*]

³¹² [assignment: *action*]

³¹³ [assignment: *Limited capability and availability policy*]

- 3490 FMT_MTD.1/AA_Private_Key
- 3491 Management of TSF data – Active Authentication Private Key

- 3492 Hierarchical to: No other components

- 3493 Dependencies: FMT_SMF.1 Specification of management functions
- 3494 fulfilled by FMT_SMF.1/EAC1PP

- 3495 FMT_SMR.1 Security roles fulfilled by
- 3496 FMT_SMR.1/PACE_EAC1PP

- 3497 FMT_MTD.1.1/AA_Private_Key

- 3498 The TSF shall restrict the ability to create or load³¹⁴ the Active Authentication Private
- 3499 Key³¹⁵ to the Personalization Agent.³¹⁶

3500 **6.1.7. Class FPT**

3501 The following security functional requirements are imported from [6], and address the

3502 protection against forced illicit information leakage, including physical manipulation.

- 3503 • **FPT_EMS.1/EAC2PP**

3504 **115. Application note (taken from [20], application note 16)**

3505 Note that related to Application Note 6 of [20], the PIN in the above SFR refers here to both

3506 the PIN for an eID application, and also the PIN for an eSign application, if they exist on card.

- 3507 • **FPT_FLS.1/EAC2PP**
- 3508 • **FPT_TST.1/EAC2PP**
- 3509 • **FPT_PHP.3/EAC2PP**

3510 The following SFRs are imported due to claiming [5]. They mostly concern the protection of

3511 security functionality related to EAC1-protected data.

- 3512 • **FPT_TST.1/EAC1PP**

3513 (equivalent to **FPT_TST.1/EAC2PP**, but listed here for the sake of completeness)

³¹⁴ [assignment: *change_default, query, modify, delete, clear, [assignment: other operations]*]

³¹⁵ [assignment: *list of TSF data*]

³¹⁶ [assignment: *the authorized identified roles*]

3514 • **FPT_FLS.1/EAC1PP**

3515 (equivalent to **FPT_FLS.1/EAC2PP**, but listed here for the sake of completeness)

3516 • **FPT_PHP.3/EAC1PP**

3517 (equivalent to **FPT_PHP.3/EAC2PP**, but listed here for the sake of completeness)

3518 • **FPT_EMS.1/EAC1PP**

3519 The following SFRs are imported due to claiming [14]. They mostly concern the protection of
 3520 security functionality related to eSign application (if available).

3521 • **FPT_EMS.1/SSCDPP**

3522 • **FPT_FLS.1/SSCDPP**

3523 (subsumed by **FPT_FLS.1/EAC2PP**)

3524 • **FPT_PHP.1/SSCDPP**

3525 • **FPT_PHP.3/SSCDPP**

3526 (subsumed by **FPT_PHP.3/EAC2PP**)

3527 • **FPT_TST.1/SSCDPP**

3528 (subsumed by **FPT_TST.1/EAC2PP**)

3529 **FPT_EMS.1/EAC2PP**

3530 TOE Emanation

3531 Hierarchical to: No other components

3532 Dependencies: No dependencies

3533 **FPT_EMS.1.1/EAC2PP**

3534 The TOE shall not emit variations in power consumption or timing during command
 3535 execution³¹⁷ in excess of non-useful information³¹⁸ enabling access to

3536 1. the session keys (PACE-K_{MAC}, PACE-K_{Enc}), (CA-K_{MAC}, CA-K_{Enc}),

³¹⁷ [assignment: *types of emissions*]

³¹⁸ [assignment: *specified limits*]

3537 2. the ephemeral private key ephem-SK_{PICC}-PACE.³¹⁹

3538 3. the Chip Authentication private keys (SK_{PICC})

3539 4. the PIN, PUK,

3540 5. none³²⁰

3541 and

3542 6. the Restricted Identification private key(s) SK_{ID}.³²¹

3543 7. none.³²²

3544 FPT_EMS.1.2/EAC2PP

3545 The TSF shall ensure any users³²³ are unable to use the following interface electronic
 3546 document's contactless/contact-based interface and circuit contacts³²⁴ to gain access to

3547 1. the session keys (PACE-K_{MAC}, PACE-K_{Enc}), (CA2-K_{MAC}, CA2-K_{Enc}),

3548 2. the ephemeral private key ephem -SK_{PICC}-PACE1,

3549 3. the Chip Authentication private key(s) (SK_{PICC}),

3550 4. the PIN, PUK,

3551 ~~5. the session keys (PACE-K_{MAC}, PACE-K_{Enc}), (CA-K_{MAC}, CA-K_{Enc})~~³²⁵

3552 6. none³²⁶

3553 and

3554 7. the Restricted Identification private key(s) SK_{ID}.³²⁷

3555 8. none.³²⁸

3556 **116. Application note (taken from [6], application note 46)**

3557 The TOE shall prevent attacks against the listed secret data where the attack is based on
 3558 external observable physical phenomena of the TOE. Such attacks may be observable at the
 3559 interfaces of the TOE, originate from internal operation of the TOE, or be caused by an attacker
 3560 that varies the physical environment under which the TOE operates. The set of measurable
 3561 physical phenomena is influenced by the technology employed to implement the smart card.
 3562 Examples of measurable phenomena include, but are not limited to variations in power

³¹⁹ [assignment: list of types of TSF data]

³²⁰ [assignment: list of types of TSF data]

³²¹ [assignment: list of types of user data]

³²² [assignment: list of types of user data]

³²³ [assignment: type of users]

³²⁴ [assignment: type of connection]

³²⁵ [assignment: list of types of TSF data]

³²⁶ [assignment: list of types of TSF data]

³²⁷ [assignment: list of types of user data]

³²⁸ [assignment: list of types of user data]

3563 consumption, timing of signals, and electromagnetic radiation due to internal operations or
 3564 data transmissions.

3565 Note that while the security functionality described in FPT_EMS.1/EAC2PP should be taken
 3566 into account during development of the TOE, associated tests must be carried out as part of
 3567 the evaluation, and not/not only during product development.

3568 Note that in the above SFR, all items in FPT_EMS.1/EAC2PP from 3. upwards are additional
 3569 assignments. The first item is slightly refined to include CA-key(s).

3570 **117. Application note (from ST author)**

3571 The PIN in the above SFR refers here to both the PIN for an eID application, and also the PIN
 3572 for an eSign application, if they exist on card.

3573 The above SFR is refined from [6] by adding all relevant key material from Chip Authentication
 3574 2, the additional assignment to cover the private sector keys. Thus, the set of keys that need
 3575 to be protected is a superset of the ones of the SFR from [6]. Hence, the requirement is stricter
 3576 than the one from [6], and the refinement operation is justified.

3577 The FPT_EMS.1.2/EAC2PP is refined because in the [20] first and fifth point is identical and
 3578 unnecessary to repeat the first point in the current ST.

3579 **FPT_FLS.1/EAC2PP**
 3580 **Failure with preservation of secure state**

3581 Hierarchical to: No other components

3582 Dependencies: No dependencies

3583 **FPT_FLS.1.1_EAC2PP**

3584 The TSF shall preserve a secure state when the following types of failures occur:

- 3585 1. Exposure to operating conditions causing a TOE malfunction,
- 3586 2. Failure detected by TSF according to FPT_TST.1,³²⁹
- 3587 3. none.³³⁰

3588 **FPT_TST.1/EAC2PP**
 3589 **TSF testing**

3590 Hierarchical to: No other components

3591 Dependencies: No dependencies

3592 **FPT_TST.1.1/EAC2PP**

³²⁹ [assignment: list of types of failures in the TSF]

³³⁰ [assignment: list of types of failures in the TSF]

3593 The TSF shall run a suite of self tests during initial start-up, periodically during normal
 3594 operation³³¹ to demonstrate the correct operation of the TSF.³³²

3595 FPT_TST.1.2/EAC2PP

3596 The TSF shall provide authorised users with the capability to verify the integrity of the TSF
 3597 data.³³³

3598 FPT_TST.1.3/EAC2PP

3599 The TSF shall provide authorised users with the capability to verify the integrity of stored
 3600 TSF executable code.³³⁴

3601 FPT_PHP.3/EAC2PP
 3602 Resistance to physical attack

3603 Hierarchical to: No other components

3604 Dependencies: No dependencies

3605 FPT_PHP.3.1_EAC2PP

3606 The TSF shall resist physical manipulation and physical probing³³⁵ to the TSF³³⁶ by
 3607 responding automatically such that the SFRs are always enforced.

3608 FPT_EMS.1/EAC1PP
 3609 TOE Emanation

3610 Hierarchical to: No other components

3611 Dependencies: No dependencies

3612 FPT_EMS.1.1/EAC1PP

3613 The TOE shall not emit variations in power consumption or timing during command
 3614 execution³³⁷ in excess of non-useful information³³⁸ enabling access to

3615 1. Chip Authentication (Version 1) Session Keys,

³³¹ [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]]

³³² [selection: [assignment: *parts of TSF*], *the TSF*]

³³³ [selection: [assignment: *parts of TSF*], *TSF data*]

³³⁴ [selection: [assignment: *parts of TSF*], *TSF*]

³³⁵ [assignment: *physical tampering scenarios*]

³³⁶ [assignment: *list of TSF devices/elements*]

³³⁷ [assignment: *types of emissions*]

³³⁸ [assignment: *specified limits*]

- 3616 2. PACE session Keys (PACE-K_{MAC}, PACE-K_{Enc}).
- 3617 3. the ephemeral private key ephem SK_{PICC-PACE}.
- 3618 4. the ephemeral private key SK_{MapPICC-PACE-CAM}³³⁹
- 3619 5. Active Authentication Private Key³⁴⁰
- 3620 6. Personalisation Agent Key(s)
- 3621 7. Chip Authentication (**Version 1**) Private Key³⁴¹ and
- 3622 8. none³⁴²

3623 FPT_EMS.1.2/EAC1PP

3624 The TSF shall ensure any users³⁴³ are unable to use the following interface smart card
 3625 circuit contacts³⁴⁴ to gain access to

- 3626 1. Chip Authentication (**Version 1**) Session Keys.
- 3627 2. PACE session Keys (PACE-K_{MAC}, PACE-K_{Enc}).
- 3628 3. the ephemeral private key ephem SK_{PICC-PACE}.
- 3629 4. the ephemeral private key SK_{MapPICC-PACE-CAM}³⁴⁵
- 3630 5. Active Authentication Private Key³⁴⁶
- 3631 6. Personalisation Agent Key(s)
- 3632 7. Chip Authentication (**Version 1**) Private Key³⁴⁷ and
- 3633 8. none.³⁴⁸

3634 **118. Application note (from ST author)**

3635 This SFR covers the definition of FPT_EMS.1 in [5] and extends it by 4. and 5. of
 3636 FPT_EMS.1.1/EAC1PP and FPT_EMS.1.2/EAC1PP. Also, 1. and 7. of both
 3637 FPT_EMS.1.1/EAC1PP and FPT_EMS.1.2/EAC1PP are slightly refined in order not to confuse
 3638 Chip Authentication 1 with Chip Authentication 2.

3639 Note that FPT_EMS.1/EAC1PP in [5] is solely concerned with Chip Authentication 1, but since
 3640 it was the first version of the protocol at the time, it was simply called 'Chip Authentication' back
 3641 then.

3642 W.r.t. PACE-CAM, note the significance of protecting SK_{Map,PICC-PACE-CAM}: Whereas when
 3643 running PACE and CA1 separately, gaining knowledge of the ephemeral key SK_{PICC-PACE}
 3644 enables the attacker to decrypt the current PACE session, an attacker that gains knowledge

³³⁹ [assignment: *list of types of TSF data*]
³⁴⁰ [assignment: *list of types of TSF data*]
³⁴¹ [assignment: *list of types of user data*]
³⁴² [assignment: *list of types of user data*]
³⁴³ [assignment: *type of users*]
³⁴⁴ [assignment: *type of connection*]
³⁴⁵ [assignment: *list of types of TSF data*]
³⁴⁶ [assignment: *list of types of TSF data*]
³⁴⁷ [assignment: *list of types of TSF data*]
³⁴⁸ [assignment: *list of types of user data*]

3645 of the ephemeral key $SK_{Map,PICC-PACE-CAM}$ can not only decrypt the session but also easily
 3646 reveal the static secret chip authentication key SK_{PICC} : Let \circ denote the group operation (i.e.
 3647 addition or multiplication), and let $i(x)$ denote the inverse of x . Since the chip sends $CA_{PICC} =$
 3648 $SK_{Map,PICC-PACE-CAM} \circ i(SK_{PICC})$ to the terminal, a malicious attacker that gains knowledge of
 3649 $SK_{Map,PICC-PACE-CAM}$ can reveal SK_{PICC} by computing $SK_{PICC} = i(CA_{PICC}) \circ SK_{Map,PICC-PACE-}$
 3650 CAM.

3651 Because of the Active Authentication is supported protocol by the TOE, the SFR is extended
 3652 with Active Authentication Private Key.

3653 [119. Application note \(taken from\[5\], application note 48\)](#)

3654 Applied.

3655 FPT_EMS.1/SSCDPP
 3656 TOE Emanation

3657 Hierarchical to: No other components

3658 Dependencies: No dependencies

3659 FPT_EMS.1.1_SSCD

3660 The TOE shall not emit variations in power consumption or timing during command
 3661 execution³⁴⁹ in excess of non-useful information³⁵⁰ enabling access to RAD³⁵¹ and SCD³⁵².

3662 FPT_EMS.1.2_SSCD

3663 The TSF shall ensure that unauthorized³⁵³ are unable to use the following interface
 3664 electrical contacts³⁵⁴ to gain access to RAD³⁵⁵ and SCD³⁵⁶.

3665 [120. Application note \(taken from \[14\], application note 18\)](#)

3666 The TOE shall prevent attacks against the SCD and other secret data where the attack is
 3667 based on external observable physical phenomena of the TOE. Such attacks may be
 3668 observable at the interfaces of the TOE or may origin from internal operation of the TOE or
 3669 may origin by an attacker that varies the physical environment under which the TOE operates.
 3670 The set of measurable physical phenomena is influenced by the technology employed to
 3671 implement the TOE. Examples of measurable phenomena are variations in the power
 3672 consumption, the timing of transitions of internal states, electromagnetic radiation due to
 3673 internal operation, radio emission.

³⁴⁹ [assignment: *types of emissions*]

³⁵⁰ [assignment: *specified limits*]

³⁵¹ [assignment: *list of types of TSF data*]

³⁵² [assignment: *list of types of user data*]

³⁵³ [assignment: *type of users*]

³⁵⁴ [assignment: *type of connection*]

³⁵⁵ [assignment: *list of types of TSF data*]

³⁵⁶ [assignment: *list of types of user data*]

3674 Due to the heterogeneous nature of the technologies that may cause such emanations,
3675 evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE
3676 is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's
3677 electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA),
3678 timing attacks, etc.

3679 FPT_PHP.1/SSCDPP
3680 Passive detection of physical attack

3681 Hierarchical to: No other components

3682 Dependencies: No dependencies

3683 FPT_PHP.1.1_SSCDPP

3684 The TSF shall provide unambiguous detection of physical tampering that might
3685 compromise the TSF.

3686 FPT_PHP.1.2_SSCDPP

3687 The TSF shall provide the capability to determine whether physical tampering with the
3688 TSF's devices or TSF's elements has occurred.

3689 **6.2.Security Assurance Requirements for the TOE**

3690 The assurance requirements for the evaluation of the TOE, its development and operating
3691 environment are to choose as the predefined assurance package EAL4 augmented by the
3692 following components:

- 3693 • ALC_DVS.2 (Sufficiency of security measures),
- 3694 • ATE_DPT.2 (Testing: security enforcing modules) and
- 3695 • AVA_VAN.5 (Advanced methodical vulnerability analysis).

3696 **6.3.Security Requirements Rationale**

3697 **6.3.1. Security Functional Requirements Rationale**

3698 The following table provides an overview for the coverage of the security functional requirements, and also gives evidence for sufficiency and
 3699 necessity of the chosen SFRs.

	OT.CA2	OT.Chip_Auth_Proof[5]	OT.Chip_Auth_Proof_PACE_CAM	OT.Chip_Auth_Proof_AA	OT.Sens_Data_Conf [5]	OT.AC_Pers_EAC2	OT.Sens_Data_EAC2	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.AC_Pers	OT.Prot_Inf_Leak	OT.RI_EAC2	OT.Non_Interfere	OT.SCD/SVD_Gen [14]	OT.Sigy_SigF ([14])	OT.Cap_Avail_Loader
Class FCS																		
FCS_CKM.1/CAM	-	-	X	-	-	-	-	X	X	X	-	-	-	-	-	-	-	-
FCS_COP.1/CAM	-	-	X	-	-	-	-	X	X	X	-	-	-	-	-	-	-	-
FCS_CKM.1/CA2	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
FCS_CKM.1/RI	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	-
FCS_CKM.1/AA	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-
FCS_COP.1/AA	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Class FIA																		
FIA_UID.1/PACE_EAC1PP	-	-	X	-	X	-	-	X	X	X	-	X	-	-	-	-	-	-
FIA_UAU.1/PACE_EAC1PP	-	-	-	X	X	-	-	X	X	X	-	X	-	-	-	-	-	-
FIA_UAU.5/PACE_EAC1PP	-	-	X	-	X	-	-	X	X	X	-	X	-	-	-	-	-	-
FIA_API.1/PACE_CAM	-	-	X	-	-	-	-	X	X	X	-	-	-	-	-	-	-	-
FIA_UAU.1/SSCDPP	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X	X	-

	OT.CA2	OT.Chip_Auth_Proof[5]	OT.Chip_Auth_Proof_PACE_CAM	OT.Chip_Auth_Proof_AA	OT.Sens_Data_Conf [5]	OT.AC_Pers_EAC2	OT.Sens_Data_EAC2	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.AC_Pers	OT.Prot_Inf_Leak	OT.RI_EAC2	OT.Non_Interfere	OT.SCD/SVD_Gen [14]	OT.Sigy_SigF ([14])	OT.Cap_Avail_Loader
FIA_UAU.4/PACE_EAC1PP	-	-	-	X	-	-	-	X	X	X	-	-	-	-	-	-	-	-
FIA_API.1/AA	-	-	-	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Class FDP																		
FDP_ACF.1/TRM	-	-	-	-	X	X	X	X	-	X	-	X	-	-	X	-	-	-
Class FMT																		
FMT_SMR.1	-	X	-	-	-	X	X	X	X	X	X	X	-	-	X	-	-	-
FMT_LIM.1/Loader	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X
FMT_LIM.2/Loader	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X
FMT_MTD.1/KEY_READ_EAC1PP	-	X	-	X	X	-	-	X	X	X	-	X	-	-	-	-	-	-
FMT_MTD.1/AA_Private_Key	-	-	X	-	-	-	-	-	-	-	-	X	-	-	-	-	-	-
Class FPT																		
FPT_EMS.1/EAC1PP	-	-	-	-	-	-	-	-	-	-	-	X	X	-	X	-	-	-
FPT_EMS.1/EAC2PP	-	-	-	-	-	X	-	-	-	-	-	-	X	-	X	-	-	-
FPT_EMS.1/SSCDPP	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-

Table 11 Coverage of Security Objectives for the TOE by SFRs

3700

3701 According to [1], tracing between SFRs and security objectives must ensure that 1) each SFR
3702 traces back to at least one security objective, and 2) that each security objective for the TOE
3703 has at least one SFR tracing to it. This is illustrated for

- 3704 1. SFRs that have been newly added or refined within this ST or [20] by checking the rows
3705 of Table 11 , and for SFRs that are merely iterated or simply included due to claims of
3706 other protection profiles by looking up the rationale of that PP
3707 2. for newly introduced security objectives in this ST or [20] by checking the non-cursive
3708 columns of Table 11 , and for the other security objectives by looking up the rationale
3709 of that PP.

3710 In other words, in Table 11 , we list only:

- 3711 • SFRs that have been newly added or refined within this ST or [20]. Mere iterations or
3712 simple inclusions due to claims of other protection profiles are not listed, however. For
3713 their coverage we refer to the respective claimed PP.
3714 • Security objectives that are newly introduced in this ST or [20], and their related SFRs.
3715 • Security objectives for the TOE that are affected by the above newly added or refined
3716 SFRs.

3717 In case an SFR was refined in order to ensure the unified terminology usage, those SFRs are
3718 not listed in Table 11 or justifies below, because these refinements have no security impacts.

3719 Analogously, we limit our justification to the above SFRs and security objectives. For other
3720 security objectives, and for the justification of security objectives w.r.t. SFRs that are included
3721 or iterated from claimed protection profiles, we refer to the detailed rationales in [5], [6] and
3722 [14].

3723 **OT.Chip_Auth_Proof_PACE_CAM** is a newly introduced security objective that aims to
3724 ensure the authenticity of the electronic document's chip by the PACE-CAM protocol, in
3725 particular in the context of an ePassport application. This is supported by **FCS_CKM.1/CAM**
3726 for cryptographic key-generation, and **FIA_API.1/PACE_CAM** and **FCS_COP.1/CAM** for the
3727 implementation itself, as well as **FIA_UID.1/PACE_EAC1PP** and
3728 **FIA_UAU.5/PACE_EAC1PP**, the latter supporting the PACE protocol.

3729 **OT.Chip_Auth_Proof_AA** is a newly introduced security objective that aims to ensure the
3730 authenticity of the electronic document's chip by the Active Authentication protocol, in
3731 particular in the context of an ePassport Application. This is supported by **FCS_CKM.1/AA** for

3732 cryptographic key generation, and **FIA_API.1/AA**, **FIA_UAU.4/PACE_EAC1PP** and
3733 **FCS_COP.1/AA** for the implementation itself. The **FMT_MTD.1/KEY_READ_EAC1PP**
3734 ensures the authenticity of the TOE, because it restricts the ability to read the Active
3735 Authentication private key to none. These do not affect the discussion of the rationale of [5].

3736 The OT.AC_Pers enforce that all TSF data can be written by authorized Personalisation Agent
3737 only and this is supported by **FMT_MTD.1/AA_Private_Key** for the Active Authentication key
3738 pair.

3739 **FIA_UAU.1/SSCDPP** is refined here in a way that the TOE supports additionally EAC2 based
3740 access control w.r.t. SSCD-related user data. This does not affect the discussion of the
3741 rationale of [14].

3742 **FDP_ACF.1/TRM** unifies the access control SFPs of **FDP_ACF.1/TRM_EAC2PP** and
3743 **FDP_ACF.1/TRM_EAC1PP**. Both access control SFPs however are maintained w.r.t.
3744 sensitive EAC1-protected data and EAC2-protected data. Thus the discussion of the rationale
3745 of [5] and [6] remains unaffected.

3746 **FMT_SMR.1/EAC1PP** and **FMT_SMR.1/EAC2PP** have been unified to FMT_SMR.1 by
3747 adding additional roles. For all security objectives affected, FMT_SMR.1 supports related roles
3748 analogously as in the discussion of the rationales of [5] and [6].

3749 The security objective OT.Cap_Avail_Loader is directly covered by the SFRs
3750 **FMT_LIM.1/Loader** and **FMT_LIM.2/Loader**, which limits the availability of the loader, as
3751 required by the objective.

3752 **FPT_EMS.1/EAC1PP** and **FPT_EMS.1/EAC2PP** together define all protected data. Since all
3753 previous data are included, the discussion of the rationales of [5] and [6] is not affected.

3754 The objective **OT.Non_Interfere** aims to ensure that no security related interferences between
3755 the implementations of the different access control mechanisms exist that allow unauthorized
3756 access of user or TSF-Data. This objective is fulfilled by enforcing the access control SFPs, in
3757 particular **FDP_ACF.1/TRM** in connection with **FDP_ACC.1/TRM_EAC1PP**. Related roles are
3758 supported by **FMT_SMR.1**. Interferences that are observable by emissions from the TOE are
3759 prevented due to **FPT_EMS.1/EAC1PP**, **FPT_EMS.1/EAC2PP**, and **FPT_EMS.1/SSCDPP**,
3760 where the set union of all defined data covers all relevant data.

3761 The security objective **OT.CA2** aims at enabling verification of the authenticity of the TOE as
3762 a whole device. This objective is mainly achieved as described in [20]. The secure generation
3763 of cryptography key pair is ensured by **FCS_CKM.1/CA2**.

3764 The security objective **OT.RI_EAC2** aims at providing a way to pseudonymously identify an
3765 electronic document holder without granting a terminal read access to sensitive user data. This
3766 objective is mainly achieved as described in [20]. The secure generation of cryptography key
3767 pair is ensured by **FCS_CKM.1/RI**.

3768 **6.3.2. Rationale for SFR's Dependencies**

3769 The dependency analysis for the security functional requirements shows that the basis for
3770 mutual support and internal consistency between all defined functional requirements is
3771 satisfied. All dependencies between the chosen functional components are analyzed, and non-
3772 dissolved dependencies are appropriately explained.

3773 The dependency analysis has directly been made within the description of each SFR in Section
3774 6.1 above. All dependencies being expected by [2] and by extended components definition in
3775 Chapter 5 are either fulfilled, or their non-fulfillment is justified.

3776 **6.3.3. Security Assurance Requirements Rationale**

3777 The current assurance package was chosen based on the predefined assurance package
3778 EAL4. This package permits a developer to gain maximum assurance from positive security
3779 engineering based on good commercial development practices which, through rigorous, do not
3780 require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level,
3781 at which it is likely to retrofit to an existing product line in an economically feasible way. EAL4
3782 is applicable in those circumstances where developers or users require a moderate to high
3783 level of independently assured security in conventional commodity TOEs and are prepared to
3784 incur additional security specific engineering costs.

3785 The selection of the component ALC_DVS.2 provides a higher assurance of the security of the
3786 electronic document's development and manufacturing, especially for the secure handling of
3787 sensitive material.

3788 The selection of the component ATE_DPT.2 provides a higher assurance than the predefined
3789 EAL4 package due to requiring the functional testing of SFR-enforcing modules.

3790 The selection of the component AVA_VAN.5 provides a higher assurance than the predefined
3791 EAL4 package, namely requiring a vulnerability analysis to assess the resistance to
3792 penetration attacks performed by an attacker possessing a high attack potential (see also
3793 Table 3, entry 'Attacker'). This decision represents a part of the conscious security policy for
3794 the electronic document required by the electronic document issuer and reflected by the
3795 current ST.

3796 The set of assurance requirements being part of EAL4 fulfills all dependencies a priori. The
3797 augmentation of EAL4 chosen comprises the following assurance components: ALC_DVS.2,
3798 ATE_DPT.2 and AVA_VAN.5. For these additional assurance components, all dependencies
3799 are met or exceeded in the EAL4 assurance package. Below we list only those assurance
3800 requirements that are additional to EAL4.

3801 ALC_DVS.2

3802 Dependencies:

3803 None

3804 ATE_DPT.2

3805 Dependencies:

3806 ADV_ARC.1, ADV_TDS.3, ATE_FUN.1

3807 fulfilled by ADV_ARC.1, ADV_TDS.3, ATE_FUN.1

3808 AVA_VAN.5

3809 Dependencies:

3810 ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1,
3811 ATE_DPT.1

3812 fulfilled by ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1,
3813 AGD_PRE.1, ATE_DPT.2

3814 **6.3.4. Security Requirements – Internal Consistency**

3815 The following part of the security requirements rationale shows that the set of security
3816 requirements for the TOE consisting of the security functional requirements (SFRs) and the

3817 security assurance requirements (SARs) are internally consistent. The analysis of the TOE's
3818 security requirements with regard to their mutual support and internal consistency
3819 demonstrates:

3820 The dependency analysis in Section 6.3.2 for the security functional requirements shows that
3821 the basis for internal consistency between all defined functional requirements is satisfied. All
3822 dependencies between the chosen functional components are analyzed and non-satisfied
3823 dependencies are appropriately justified.

3824 All subjects and objects addressed by more than one SFR are also treated in a consistent way:
3825 the SFRs impacting them do not require any contradictory property or behavior of these
3826 'shared' items.

3827 The assurance package EAL4 is a predefined set of internally consistent assurance
3828 requirements. The dependency analysis for the sensitive assurance components in Section
3829 6.3.3 shows that the assurance requirements are internally consistent as all (additional)
3830 dependencies are satisfied and no inconsistency appears.

3831 Inconsistency between functional and assurance requirements can only arise due to
3832 functional-assurance dependencies not being met. As shown in Section 6.3.2 and Section
3833 6.3.3, the chosen assurance components are adequate for the functionality of the TOE. Hence,
3834 there are no inconsistencies between the goals of these two groups of security requirements.

3835 **7. TOE SUMMARY SPECIFICATION**

3836 **7.1.TOE Security Functions**

3837 **7.1.1. TSF.AccessControl**

3838 The TOE enforces access control in order to access User Data and TSF-data and maintains
 3839 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.

3840 **7.1.2. TSF.Authenticate**

3841 The TOE supports several authentication mechanism in order to authenticate the Users,
3842 Terminals and to prove the genuineness of the electronic document.

3843 The supported mechanism and protocols are based on ICAO and BSI standards [7], [8], [16],
3844 [17] and [18].

3845 Supported authentication mechanism:

- 3846 • Password Authenticated Connection Establishment (PACE) [7], [16], [17].
 - 3847 ○ Generic Mapping
 - 3848 ○ Chip Authentication Mapping
- 3849 • Active Authentication [7]
- 3850 • Chip Authentication version 1 [16]
- 3851 • Terminal Authentication version 1 [16]
- 3852 • Chip Authentication version 2 [17]
- 3853 • Terminal Authentication version 2 [17]
- 3854 • Restricted Identification [17]
- 3855 • Symmetric Authentication (Device authentication) [30]
- 3856 • Symmetric Role Authentication [30]
- 3857 • User Verification [30]

SFR	Description
FIA_AFL.1/Suspend_PIN_EAC2PP	This TSF responsible for PACE.
FIA_AFL.1/Block_PIN_EAC2PP	This TSF responsible for PACE.
FIA_API.1/CA_EAC2PP	This TSF responsible for Chip Authentication v2.
FIA_API.1/RI_EAC2PP	This TSF responsible for Restricted Identification.
FIA_UID.1/PACE_EAC2PP	This TSF responsible for PACE.
FIA_UID.1/EAC2_Terminal_EAC2PP	This TSF responsible for PACE.
FIA_UAU.1/PACE_EAC2PP	This TSF responsible for PACE.
FIA_UAU.1/EAC2_Terminal_EAC2PP	This TSF responsible for PACE and Terminal Authentication v2.
FIA_UAU.4/PACE_EAC2PP	This TSF responsible for PACE, Terminal Authentication v2 and Symmetric Authentication.
FIA_UAU.5/PACE_EAC2PP	This TSF responsible for PACE, Terminal Authentication v2, Chip Authentication v2 and Symmetric Authentication.
FIA_UAU.6/CA_EAC2PP	This TSF responsible for Chip Authentication v2.
FIA_AFL.1/PACE_EAC2PP	This TSF responsible for PACE.
FIA_UAU.6/PACE_EAC2PP	This TSF responsible for PACE.
FIA_UID.1/PACE_EAC1PP	This TSF responsible for PACE, Chip Authentication v1 and Chip Authentication Mapping (PACE-CAM).
FIA_UAU.1/PACE_EAC1PP	This TSF responsible for PACE, Chip Authentication v1, Terminal Authentication v1 and Chip Authentication Mapping (PACE-CAM).
FIA_UAU.4/PACE_EAC1PP	This TSF responsible for PACE, Symmetric Authentication, Terminal Authentication v1 and Active Authentication.
FIA_UAU.5/PACE_EAC1PP	This TSF responsible for PACE, Chip Authentication Mapping (PACE-CAM), Symmetric Authentication, Terminal Authentication v1.
FIA_UAU.6/EAC_EAC1PP	This TSF responsible for Chip Authentication v1
FIA_API.1/EAC1PP	This TSF responsible for Chip Authentication v1
FIA_API.1/PACE_CAM	This TSF responsible for Chip Authentication Mapping
FIA_API.1/AA	This TSF responsible for Active Authentication
FIA_AFL.1/PACE_EAC1PP	Equivalent to FIA_AFL.1/PACE_EAC2PP.
FIA_UAU.6/PACE_EAC1PP	This TSF responsible for PACE.
FIA_AFL.1/SSCDPP	This TSF responsible for User Verification.
FDP_ACF.1/TRM	This TSF responsible for Terminal Authentication and PACE.
FDP_ACF.1/SCD/SVD_Generation_SSCDPP	This TSF responsible for User Verification

FDP_ACF.1/SVD_Transfer_SSCDPP	This TSF responsible for R.Admin.
FDP_ACF.1/Signature-creation_SSCDPP	This TSF responsible for User Verification.
FTP_ITC.1/PACE_EAC2PP	This TSF responsible for PACE
FTP_ITC.1/CA_EAC2PP	This TSF responsible for Chip Authentication v2
FTP_ITC.1/PACE_EAC1PP	This TSF responsible for PACE.
FMT_MTD.1/CVCA_INI_EAC2PP	This TSF responsible for authentication of the Personalisation Agent.
FMT_MTD.1/CVCA_UPD_EAC2PP	This TSF responsible for the authentication of Country Verifying Certification Authority.
FMT_MTD.1/DATE_EAC2PP	This TSF responsible for the authentication of CVCA, DV and the EAC2 Terminal
FMT_MTD.1/PA_EAC2PP	This TSF responsible for authentication of Personalization Agent.
FMT_MTD.1/SK_PICC_EAC2PP	This TSF responsible for authentication of the Personalisation Agent.
FMT_MTD.1/Initialize_PIN_EAC2PP	This TSF responsible for authentication of the Personalisation Agent.
FMT_MTD.1/Change_PIN_EAC2PP	This TSF responsible for authentication of Document Holder and the EAC2 Terminal (with Terminal Authorisation level for PIN management).
FMT_MTD.1/Resume_PIN_EAC2PP	This TSF responsible for authentication of Document Holder
FMT_MTD.1/Unblock_PIN_EAC2PP	This TSF responsible for authentication of Document Holder and the EAC2 Terminal (with Terminal Authorisation level for PIN management).
FMT_MTD.1/Activate_PIN_EAC2PP	This TSF responsible for authentication of the EAC2 Terminal (with Terminal Authorisation level for PIN management).
FMT_MTD.3/EAC2PP	This TSF responsible for the Terminal Authentication v2.
FMT_SMF.1/SSCDPP	This TSF responsible to provide the security functions.
FMT_MOF.1/SSCDPP	This TSF responsible for authentication of R.Sigy
FMT_MSA.1/Admin_SSCDPP	This TSF responsible for authentication of R.Admin
FMT_MSA.1/SignatorySSCDPP	This TSF responsible for authentication of R.Sigy
FMT_MSA.3/SSCDPP	This TSF responsible for authentication of R.Sigy and R.Admin
FMT_MSA.4/SSCDPP	This TSF responsible for authentication of R.Sigy and R.Admin
FMT_MTD.1/Admin_SSCDPP	This TSF responsible for authentication of R.Admin
FMT_MTD.1/Signatory_SSCDPP	This TSF responsible for authentication of R.Sigy
FMT_MTD.1/CVCA_INI_EAC1PP	This TSF responsible for authentication of Personalization Agent.
FMT_MTD.1/CVCA_UPD_EAC1PP	This TSF responsible for authentication of Country Verifying Certification Authority.
FMT_MTD.1/DATE_EAC1PP	This TSF responsible to equivalent to FMT_MTD.1/DATE_EAC2PP.
FMT_MTD.1/CAPK_EAC1PP	This TSF responsible for This TSF responsible for authentication of Personalization Agent or the Manufacturer.
FMT_MTD.1/PA_EAC1PP	This TSF responsible for authentication of Personalization Agent.
FMT_MTD.1/AA_Private_Key	This TSF responsible for authentication of Personalization Agent.
FMT_MTD.3/EAC1PP	This TSF responsible for the Terminal Authentication v2.

3858 **7.1.3. TSF.SecureManagement**

3859 The TOE enforces the secure management of the security attributes, data and functions.
 3860 Furthermore the TOE restricts the available commands in each TOE life-cycle phase.

SFR	Description
FMT_MTD.1/CVCA_INI_EAC2PP	This TSF responsible to evaluate whether the Personalisation Agent is authenticated, and it has right to write initial CVCA Public Key, meta-data of the initial CVCA Certificate and initial Current Date.
FMT_MTD.1/CVCA_UPD_EAC2PP	This TSF responsible to evaluate whether the Country Verifying Certification Authority is authenticated, and it has right to update CVCA Public Key (PKCVCA) and meta-data of the CVCA Certificate.
FMT_SMF.1/EAC2PP	This TSF responsible to provide part of the security functions.
FMT_MTD.1/DATE_EAC2PP	This TSF responsible to evaluate whether a CVCA, Document Verifier, or an EAC2 terminal is authenticated and it has right to modify Current Date.
FMT_MTD.1/PA_EAC2PP	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to write the card/chip security object(s) (SO _C) and the document Security Object (SO _D).
FMT_MTD.1/SK_PICC_EAC2PP	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to create or load the Chip Authentication private key(s) (SKPICC) and the Restricted Identification Private Key(s).
FMT_MTD.1/KEY_READ_EAC2PP	This TSF responsible to restrict the ability to read certain objects.
FMT_MTD.1/Initialize_PIN_EAC2PP	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to write the initial PIN and PUK
FMT_MTD.1/Change_PIN_EAC2PP	This TSF responsible to evaluate whether an Electronic Document Holder is authenticated with PUK or a Terminal with Terminal Authorisation level for PIN management is authenticated and it has right to change the blocked PIN.
FMT_MTD.1/Resume_PIN_EAC2PP	This TSF responsible to evaluate whether an Electronic Document Holder is authenticated, and it has right to resume the suspended PIN.
FMT_MTD.1/Unblock_PIN_EAC2PP	This TSF responsible to evaluate whether an Electronic Document Holder is authenticated with PUK or a Terminal with Terminal Authorisation level for PIN management is authenticated and it has right to unblock the blocked PIN.
FMT_MTD.1/Activate_PIN_EAC2PP	This TSF responsible to evaluate whether a Terminal with Terminal Authorisation level for PIN management is authenticated and it has right to activate or deactivate the PIN.
FMT_SMF.1/SSCDPP	This TSF responsible to provide part of the security functions.
FMT_MOF.1/SSCDPP	This TSF responsible to evaluate whether a R.Sigy is authenticated and it has right to enable the signature creation function.
FMT_MSA.1/Admin_SSCDPP	This TSF responsible to evaluate whether a R.Admin is authenticated and it has right to modify the SCD/SVD management security attribute.

FMT_MSA.1/SignatorySSCDPP	This TSF responsible to evaluate whether a R.Sigy is authenticated and it has right to modify the SCD/SVD operational security attribute.
FMT_MSA.2/SSCDPP	This TSF responsible to ensure that only secure values are accepted for SCD/SVD Management and SCD operational
FMT_MSA.3/SSCDPP	This TSF responsible to provide restrictive default values for security attributes.
FMT_MSA.4/SSCDPP	This TSF responsible for security attribute value inheritance.
FMT_MTD.1/Admin_SSCDPP	This TSF responsible to evaluate whether a R.Admin is authenticated, and it has right to create the RAD.
FMT_MTD.1/Signatory_SSCDPP	This TSF responsible to evaluate whether a R.Sigy is authenticated and it has right to modify the RAD.
FMT_MTD.1/CVCA_INI_EAC1PP	This TSF responsible to evaluate whether the Personalisation Agent is authenticated, and it has right to write initial Country Verifying Certification Authority Public Key, initial Country Verifying Certification Authority Certificate, initial Current Date.
FMT_MTD.1/CVCA_UPD_EAC1PP	This TSF responsible to evaluate whether the Country Verifying Certification Authority is authenticated, and it has right to update Country Verifying Certification Authority Public Key, Country Verifying Certification Authority Certificate.
FMT_SMF.1/EAC1PP	This TSF responsible to provide part of the security functions.
FMT_MTD.1/DATE_EAC1PP	This TSF responsible to equivalent to FMT_MTD.1/DATE_EAC2PP.
FMT_MTD.1/CAPK_EAC1PP	This TSF responsible to evaluate whether a Personalisation Agent or Manufacturer is authenticated, and it has right to create or load the Chip Authentication private key.
FMT_MTD.1/PA_EAC1PP	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to write the document Security Object (SOD).
FMT_MTD.1/KEY_READ_EAC1PP	This TSF responsible to restrict the ability to read cryptographic keys.
FMT_MTD.1/AA_Private_Key	This TSF responsible to evaluate whether a Personalisation Agent is authenticated, and it has right to create or load the Active Authentication Private Key.

3861 **7.1.4. TSF.CryptoKey**

3862 The TOE uses several cryptographic services such as digital signature creation and
 3863 verification, asymmetric and symmetric cryptography, random number generation and
 3864 complete key management.

3865 Furthermore TSF.CryptoKey provides the secure messaging for the TOE.

SFR	Description
FCS_CKM.1/DH_PACE_EAC2PP	This TSF responsible the Applet part of key agreement for PACE.
FCS_COP.1/SHA_EAC2PP	This TSF responsible the Applet part of hash generation.
FCS_COP.1/SIG_VER_EAC2PP	This TSF responsible the Applet part of digital signature verification.
FCS_COP.1/PACE_ENC_EAC2PP	This TSF responsible the Applet part of secure messaging – encryption and decryption.
FCS_COP.1/PACE_MAC_EAC2PP	This TSF responsible the Applet part of secure messaging – message authentication code.

FCS_CKM.4/EAC2PP	This TSF responsible the Applet part of cryptographic key destruction.
FCS_RND.1/EAC2PP	This TSF responsible the Applet part of random number generation.
FCS_CKM.1/DH_PACE_EAC1PP	This TSF responsible the Applet part of key agreement for PACE.
FCS_CKM.4/EAC1PP	Equivalent to FCS_CKM.4/EAC2PP.
FCS_COP.1/PACE_ENC_EAC1PP	This TSF responsible the Applet part of secure messaging – encryption and decryption.
FCS_COP.1/PACE_MAC_EAC1PP	This TSF responsible the Applet part of secure messaging – message authentication code.
FCS_RND.1/EAC1PP	Equivalent to FCS_RND.1/EAC2PP.
FCS_CKM.1/CA_EAC1PP	This TSF responsible the Applet part of key agreement for Chip Authentication v1.
FCS_COP.1/CA_ENC_EAC1PP	This TSF responsible the Applet part of secure messaging – encryption and decryption.
FCS_COP.1/SIG_VER_EAC1PP	This TSF responsible the Applet part of digital signature verification.
FCS_COP.1/CA_MAC_EAC1PP	This TSF responsible the Applet part of secure messaging – message authentication code.
FCS_CKM.1/CA2	This TSF responsible the Applet part of Chip Authentication version 2 Key pair(s) generation.
FCS_CKM.1/RI	This TSF responsible the Applet part of Restricted Identification Key pair (s) generation.
FCS_CKM.1/AA	This TSF responsible the Applet part of Active Authentication Key Pair generation.
FCS_COP.1/AA	This TSF responsible the Applet part of digital signature generation.
FCS_CKM.1/CAM	This TSF responsible the Applet part of PACE-CAM protocol implementation.
FCS_COP.1/CAM	This TSF responsible the Applet part of PACE-CAM protocol implementation.
FCS_CKM.1/SSCDPP	This TSF responsible the Applet part of SCD/SVD pair generation.
FCS_COP.1/SSCDPP	This TSF responsible the Applet part of digital signature creation.
FIA_API.1/CA_EAC2PP	This TSF responsible the Applet part of cryptographic operation for Chip Authentication v2.
FIA_API.1/RI_EAC2PP	This TSF responsible the Applet part of cryptographic operation for Restricted Identification.
FIA_API.1/EAC1PP	This TSF responsible the Applet part of cryptographic operation for Chip Authentication v1.
FIA_API.1/PACE_CAM	This TSF responsible the Applet part of cryptographic operation for Chip Authentication Mapping.
FIA_API.1/AA	This TSF responsible the Applet part of cryptographic operation for Active Authentication.
FDP_RIP.1/EAC2PP	This TSF responsible to call the Platform functionalities to destroy cryptographic keys.
FDP_UCT.1/TRM_EAC2PP	This TSF responsible the Applet part of secure messaging.
FDP_UIT.1/TRM_EAC2PP	This TSF responsible the Applet part of secure messaging.
FDP_RIP.1/EAC1PP	This TSF responsible to call the Platform functionalities to destroy cryptographic keys.
FDP_UCT.1/TRM_EAC1PP	Equivalent to FDP_UCT.1/TRM_EAC2PP.
FDP_UIT.1/TRM_EAC1PP	Equivalent to FDP_UIT.1/TRM_EAC2PP.
FDP_RIP.1/SSCDPP	This TSF responsible the Applet part of de-allocation of the resource SCD.
FTP_ITC.1/PACE_EAC2PP	This TSF responsible the Applet part of cryptographic operation for trusted channel.

FTP_ITC.1/CA_EAC2PP	This TSF responsible the Applet part of cryptographic operation for trusted channel.
FTP_ITC.1/PACE_EAC1PP	This TSF responsible the Applet part of cryptographic operation for trusted channel.

3866 **7.1.5. TSF.AppletParametersSign**

3867 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.

3868 **7.1.6. TSF.Platform**

3869 The TOE relies on the certified functions and services of the Platform. This TSF is collection
3870 of those SFRs, which are uses these functions and services.

SFR	Description
FCS_CKM.1/DH_PACE_EAC2PP	This TSF responsible the Platform part of key agreement for PACE.
FCS_COP.1/SHA_EAC2PP	This TSF responsible the Platform part of hash generation.
FCS_COP.1/SIG_VER_EAC2PP	This TSF responsible the Platform part of digital signature verification.
FCS_COP.1/PACE_ENC_EAC2PP	This TSF responsible the Platform part of secure messaging – encryption and decryption.
FCS_COP.1/PACE_MAC_EAC2PP	This TSF responsible the Platform part of secure messaging – message authentication code.
FCS_CKM.4/EAC2PP	This TSF responsible the Platform part of cryptographic key destruction.
FCS_RND.1/EAC2PP	This TSF responsible the Platform part of random number generation.
FCS_CKM.1/DH_PACE_EAC1PP	This TSF responsible the Platform part of key agreement for PACE.
FCS_CKM.4/EAC1PP	Equivalent to FCS_CKM.4/EAC2PP.
FCS_COP.1/PACE_ENC_EAC1PP	This TSF responsible the Platform part of secure messaging – encryption and decryption.
FCS_COP.1/PACE_MAC_EAC1PP	This TSF responsible the Platform part of secure messaging – message authentication code.
FCS_RND.1/EAC1PP	Equivalent to FCS_RND.1/EAC2PP.
FCS_CKM.1/CA_EAC1PP	This TSF responsible the Platform part of key agreement for Chip Authentication v1.
FCS_COP.1/CA_ENC_EAC1PP	This TSF responsible the Platform part of secure messaging – encryption and decryption.
FCS_COP.1/SIG_VER_EAC1PP	This TSF responsible the Platform part of digital signature verification.
FCS_COP.1/CA_MAC_EAC1PP	This TSF responsible the Platform part of secure messaging – message authentication code.
FCS_CKM.1/CA2	This TSF responsible the Platform part of Chip Authentication version 2 Key pair(s) generation.
FCS_CKM.1/RI	This TSF responsible the Platform part of Restricted Identification Key pair(s) generation.
FCS_CKM.1/AA	This TSF responsible the Platform part of Active Authentication Key Pair generation.

FCS_COP.1/AA	This TSF responsible the Platform part of digital signature generation.
FCS_CKM.1/CAM	This TSF responsible the Platform part of PACE-CAM protocol implementation.
FCS_COP.1/CAM	This TSF responsible the Platform part of PACE-CAM protocol implementation.
FCS_CKM.1/SSCDPP	This TSF responsible the Platform part of SCD/SVD pair generation.
FCS_CKM.4/SSCDPP	This TSF responsible the Platform part of cryptographic key destruction.
FCS_COP.1/SSCDPP	This TSF responsible the Platform part of digital signature creation.
FIA_API.1/CA_EAC2PP	This TSF responsible the Platform part of cryptographic operation for Chip Authentication v2.
FIA_API.1/RI_EAC2PP	This TSF responsible the Platform part of cryptographic operation for Restricted Identification.
FIA_UID.1/PACE_EAC2PP	This TSF responsible for the identifier data of the TOE.
FIA_UID.1/EAC2_Terminal_EAC2PP	This TSF responsible for the identifier data of the TOE.
FIA_UAU.1/PACE_EAC2PP	This TSF responsible for the identifier data of the TOE.
FIA_UAU.1/EAC2_Terminal_EAC2PP	This TSF responsible for the identifier data of the TOE.
FIA_UID.1/PACE_EAC1PP	This TSF responsible for the identifier data of the TOE.
FIA_UAU.1/PACE_EAC1PP	This TSF responsible for the identifier data of the TOE.
FIA_UAU.4/PACE_EAC2PP	This TSF responsible for fresh random numbers for PACE, Terminal Authentication v2 and Symmetric Authentication.
FIA_UAU.5/PACE_EAC2PP	This TSF responsible for Platform part of cryptographic operation for PACE, Terminal Authentication v2, Chip Authentication v2 and Symmetric Authentication.
FIA_UAU.6/CA_EAC2PP	This TSF responsible for Platform part of cryptographic operation for Chip Authentication v2.
FIA_UAU.6/PACE_EAC2PP	This TSF responsible for Platform part of cryptographic operation for PACE.
FIA_UAU.4/PACE_EAC1PP	This TSF responsible for Platform part of cryptographic operation for PACE, Symmetric Authentication, Terminal Authentication v1 and Active Authentication.
FIA_UAU.5/PACE_EAC1PP	This TSF responsible for Platform part of cryptographic operation for PACE, Chip Authentication Mapping (PACE-CAM), Symmetric Authentication, Terminal Authentication v1.
FIA_UAU.6/PACE_EAC1PP	This TSF responsible for Platform part of cryptographic operation for PACE.
FIA_UAU.6/EAC_EAC1PP	This TSF responsible for Platform part of cryptographic operation for Chip Authentication v1
FIA_API.1/EAC1PP	This TSF responsible the Platform part of cryptographic operation for Chip Authentication v1.
FIA_API.1/PACE_CAM	This TSF responsible the Platform part of cryptographic operation for Chip Authentication Mapping.
FIA_API.1/AA	This TSF responsible the Platform part of cryptographic operation for Active Authentication.
FDP_RIP.1/EAC2PP	This TSF responsible to make unavailable any cryptographic data used in runtime cryptographic computations.
FDP_UCT.1/TRM_EAC2PP	This TSF responsible the Platform part of secure messaging.
FDP_UIT.1/TRM_EAC2PP	This TSF responsible the Platform part of secure messaging.
FDP_RIP.1/EAC1PP	This TSF responsible to make unavailable any cryptographic data used in runtime cryptographic computations.
FDP_UCT.1/TRM_EAC1PP	Equivalent to FDP_UCT.1/TRM_EAC2PP.

FDP_UIT.1/TRM_EAC1PP	Equivalent to FDP_UIT.1/TRM_EAC2PP.
FDP_RIP.1/SSCDPP	This TSF responsible the Platform part of de-allocation of the resource SCD.
FDP_SDI.2/Persistent_SSCDPP	This TSF responsible for integrity of user data.
FDP_SDI.2/DTBS_SSCDPP	This TSF responsible for integrity of user data.
FAU_SAS.1/EAC2PP	This TSF responsible to store the Initialisation and Pre-Personalisation Data in the audit records
FAU_SAS.1/EAC1PP	Equivalent to FAU_SAS.1/EAC2PP.
FMT_SMR.1	This TSF responsible to provide part of the security roles.
FMT_LIM.1/EAC2PP	This TSF responsible to limit its capabilities to enforce the policy as described in the SFR.
FMT_LIM.2/EAC2PP	This TSF responsible to limit its availability to enforce the policy as described in the SFR.
FMT_MTD.1/INI_ENA_EAC2PP	This TSF responsible to restrict the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer.
FMT_MTD.1/INI_DIS_EAC2PP	This TSF responsible to restrict the ability to read out the Initialisation Data and the Pre-personalisation Data to the Personalisation Agent.
FMT_SMF.1/EAC2PP	This TSF responsible to provide part of the security functions.
FMT_SMF.1/EAC1PP	This TSF responsible to provide part of the security functions.
FMT_LIM.1/EAC1PP	Equivalent to FMT_LIM.1/EAC2PP.
FMT_LIM.2/EAC1PP	Equivalent to FMT_LIM.2/EAC2PP.
FMT_MTD.1/INI_ENA_EAC1PP	Equivalent to FMT_MTD.1/INI_ENA_EAC2PP.
FMT_MTD.1/INI_DIS_EAC1PP	Equivalent to FMT_MTD.1/INI_DIS_EAC2PP.
FPT_EMS.1/EAC2PP	This TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timing (measurable at e. g. electrical contacts) that might disclose cryptographic keys.
FPT_FLS.1/EAC2PP	This TSF responsible to preserve a secure state when the failures occur.
FPT_TST.1/EAC2PP	This TSF responsible for the integrity of stored TSF executable code.
FPT_PHP.3/EAC2PP	This TSF ensures resistance to physical attack.
FPT_TST.1/EAC1PP	Equivalent to FPT_TST.1/EAC2PP.
FPT_FLS.1/EAC1PP	Equivalent to FPT_FLS.1/EAC2PP.
FPT_PHP.3/EAC1PP	Equivalent to FPT_PHP.3/EAC2PP
FPT_EMS.1/EAC1PP	This TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timing (measurable at e. g. electrical contacts) that might disclose cryptographic keys.
FPT_EMS.1/SSCDPP	This TSF ensures that during command execution there are no usable variations in power consumption (measurable at e. g. electrical contacts) or timing (measurable at e. g. electrical contacts) that might disclose cryptographic keys.
FPT_FLS.1/SSCDPP	Equivalent to FPT_FLS.1/EAC2PP.
FPT_PHP.1/SSCDPP	This TSF ensures the passive detection of physical attack.
FPT_PHP.3/SSCDPP	Subsumed by FPT_PHP.3/EAC2PP.
FPT_TST.1/SSCDPP	Subsumed by FPT_TST.1/EAC2PP.
FMT_LIM.1/Loader	This TSF responsible to limit its capabilities to enforce the policy as described in the SFR.

FMT_LIM.2/Loader	This TSF responsible to limit its availability to enforce the policy as described in the SFR.
-------------------------	---

3871 **7.2.Assurance Measures**

3872 This section describes the Assurance Measures fulfilling the requirements listed in section 6.2.

3873 The following table lists the Assurance measures and references the corresponding

3874 documents describing the measures.

Assurance measures	Description
AM_ADV	The representing of the TSF is described in the documentation for functional specification, in the documentation for TOE design, in the security architecture description and in the documentation for implementation representation.
AM_AGD	The guidance documentation is described in the User’s Guide documentation [22] and the Administrator’s Guide documentation [21].
AM_ALC	The life-cycle support of the TOE during its development and maintenance is described in the life-cycle documentation including configuration management, delivery procedures, development security as well as development tools.
AM_ATE	The testing of the TOE is described in the test documentation.
AM_AVA	The vulnerability assessment for the TOE is described in the vulnerability analysis documentation.

3875 **Table 12 Assurance measures and corresponding documents**

3876 **7.3.Fulfillment of the SFRs**

3877 The following table shows the mapping of the SFRs to security functions of the TOE:

TOE SFR / Security Function						
	TSF.AccessControl	TSF.Authenticate	TSF.SecureManagement	TSF.CryptoKey	TSF.AppletParametersSign	TSF.Platform
FCS_CKM.1/DH_PACE_EAC2PP	-	-	-	X	-	X
FCS_COP.1/SHA_EAC2PP	-	-	-	X	-	X
FCS_COP.1/SIG_VER_EAC2PP	-	-	-	X	-	X
FCS_COP.1/PACE_ENC_EAC2PP	-	-	-	X	-	X
FCS_COP.1/PACE_MAC_EAC2PP	-	-	-	X	-	X
FCS_CKM.4/EAC2PP	-	-	-	X	-	X
FCS_RND.1/EAC2PP	-	-	-	X	-	X
FCS_CKM.1/DH_PACE_EAC1PP	-	-	-	X	-	X
FCS_CKM.4/EAC1PP	-	-	-	X	-	X
FCS_COP.1/PACE_ENC_EAC1PP	-	-	-	X	-	X
FCS_COP.1/PACE_MAC_EAC1PP	-	-	-	X	-	X
FCS_RND.1/EAC1PP	-	-	-	X	-	X
FCS_CKM.1/CA_EAC1PP	-	-	-	X	-	X
FCS_COP.1/CA_ENC_EAC1PP	-	-	-	X	-	X
FCS_COP.1/SIG_VER_EAC1PP	-	-	-	X	-	X
FCS_COP.1/CA_MAC_EAC1PP	-	-	-	X	-	X
FCS_CKM.1/CA2	-	-	-	X	-	X
FCS_CKM.1/RI	-	-	-	X	-	X
FCS_CKM.1/AA	-	-	-	X	-	X
FCS_COP.1/AA	-	-	-	X	-	X
FCS_CKM.1/CAM	-	-	-	X	-	X
FCS_COP.1/CAM	-	-	-	X	-	X
FCS_CKM.1/SSCDPP	-	-	-	X	-	X
FCS_COP.1/SSCDPP	-	-	-	X	-	X
FIA_AFL.1/Suspend_PIN_EAC2PP	X	X	-	-	-	-
FIA_AFL.1/Block_PIN_EAC2PP	X	X	-	-	-	-
FIA_API.1/CA_EAC2PP	-	X	-	X	-	X
FIA_API.1/RI_EAC2PP	-	X	-	X	-	X
FIA_UID.1/PACE_EAC2PP	X	X	-	-	-	X
FIA_UID.1/EAC2_Terminal_EAC2PP	X	X	-	-	-	X
FIA_UAU.1/PACE_EAC2PP	X	X	-	-	-	X
FIA_UAU.1/EAC2_Terminal_EAC2PP	X	X	-	-	-	X
FIA_UAU.4/PACE_EAC2PP	-	X	-	-	-	X
FIA_UAU.5/PACE_EAC2PP	-	X	-	-	-	X
FIA_UAU.6/CA_EAC2PP	-	X	-	-	-	X
FIA_AFL.1/PACE_EAC2PP	X	X	-	-	-	-

TOE SFR / Security Function	TSF					
	AccessControl	Authenticate	SecureManagement	CryptoKey	AppletParametersSign	Platform
FIA_UAU.6/PACE_EAC2PP	-	X	-	-	-	X
FIA_UID.1/PACE_EAC1PP	X	X	-	-	-	X
FIA_UAU.1/PACE_EAC1PP	X	X	-	-	-	X
FIA_UAU.4/PACE_EAC1PP	-	X	-	-	-	X
FIA_UAU.5/PACE_EAC1PP	-	X	-	-	-	X
FIA_UAU.6/PACE_EAC1PP	-	X	-	-	-	X
FIA_UAU.6/EAC_EAC1PP	-	X	-	-	-	X
FIA_API.1/EAC1PP	-	X	-	X	-	X
FIA_API.1/PACE_CAM	-	X	-	X	-	X
FIA_API.1/AA	-	X	-	X	-	X
FIA_AFL.1/PACE_EAC1PP	X	X	-	-	-	-
FIA_UID.1/SSCDPP	X	-	-	-	-	-
FIA_AFL.1/SSCDPP	X	X	-	-	-	-
FIA_UAU.1/SSCDPP	X	-	-	-	-	-
FDP_ACC.1/TRM_EAC2PP	X	-	-	-	-	-
FDP_ACF.1/TRM	X	X	-	-	-	-
FDP_RIP.1/EAC2PP	-	-	-	X	-	X
FDP_UCT.1/TRM_EAC2PP	-	-	-	X	-	X
FDP_UIT.1/TRM_EAC2PP	-	-	-	X	-	X
FDP_ACC.1/TRM_EAC1PP	X	-	-	-	-	-
FDP_RIP.1/EAC1PP	-	-	-	X	-	X
FDP_UCT.1/TRM_EAC1PP	-	-	-	X	-	X
FDP_UIT.1/TRM_EAC1PP	-	-	-	X	-	X
FDP_ACC.1/SCD/SVD_Generation_SSCDPP	X	-	-	-	-	-
FDP_ACF.1/SCD/SVD_Generation_SSCDPP	X	X	-	-	-	-
FDP_ACC.1/SVD_Transfer_SSCDPP	X	-	-	-	-	-
FDP_ACF.1/SVD_Transfer_SSCDPP	X	X	-	-	-	-
FDP_ACC.1/Signature-creation_SSCDPP	X	-	-	-	-	-
FDP_ACF.1/Signature-creation_SSCDPP	X	X	-	-	-	-
FDP_RIP.1/SSCDPP	-	-	-	X	-	X
FDP_SDI.2/Persistent_SSCDPP	-	-	-	-	-	X
FDP_SDI.2/DTBS_SSCDPP	-	-	-	-	-	X
FTP_ITC.1/PACE_EAC2PP	-	X	-	X	-	-
FTP_ITC.1/CA_EAC2PP	-	X	-	X	-	-
FTP_ITC.1/PACE_EAC1PP	-	X	-	X	-	-
FAU_SAS.1/EAC2PP	-	-	-	-	-	X
FAU_SAS.1/EAC1PP	-	-	-	-	-	X
FMT_MTD.1/CVCA_INI_EAC2PP	X	X	X	-	-	-

TOE SFR / Security Function	TSF.AccessControl	TSF.Authenticate	TSF.SecureManagement	TSF.CryptoKey	TSF.AppletParametersSign	TSF.Platform
FMT_MTD.1/CVCA_UPD_EAC2PP	X	X	X	-	-	-
FMT_SMF.1/EAC2PP	-	-	X	-	-	X
FMT_SMR.1	X	-	-	-	-	X
FMT_MTD.1/DATE_EAC2PP	X	X	X	-	-	-
FMT_MTD.1/PA_EAC2PP	X	X	X	-	-	-
FMT_MTD.1/SK_PICC_EAC2PP	X	X	X	-	-	-
FMT_MTD.1/KEY_READ_EAC2PP	X	-	X	-	-	-
FMT_MTD.1/Initialize_PIN_EAC2PP	-	X	X	-	-	-
FMT_MTD.1/Change_PIN_EAC2PP	-	X	X	-	-	-
FMT_MTD.1/Resume_PIN_EAC2PP	-	X	X	-	-	-
FMT_MTD.1/Unblock_PIN_EAC2PP	-	X	X	-	-	-
FMT_MTD.1/Activate_PIN_EAC2PP	-	X	X	-	-	-
FMT_MTD.3/EAC2PP	-	X	-	-	-	-
FMT_SMR.1/SSCDPP	X	-	-	-	-	-
FMT_SMF.1/SSCDPP	-	X	X	-	-	-
FMT_MOF.1/SSCDPP	X	X	X	-	-	-
FMT_MSA.1/Admin_SSCDPP	X	X	X	-	-	-
FMT_MSA.1/SignatorySSCDPP	X	X	X	-	-	-
FMT_MSA.2/SSCDPP	-	-	X	-	-	-
FMT_MSA.3/SSCDPP	X	X	X	-	-	-
FMT_MSA.4/SSCDPP	-	X	X	-	-	-
FMT_MTD.1/Admin_SSCDPP	X	X	X	-	-	-
FMT_MTD.1/Signatory_SSCDPP	X	X	X	-	-	-
FMT_LIM.1/EAC2PP	-	-	-	-	-	X
FMT_LIM.2/EAC2PP	-	-	-	-	-	X
FMT_MTD.1/INI_ENA_EAC2PP	-	-	-	-	-	X
FMT_MTD.1/INI_DIS_EAC2PP	-	-	-	-	-	X
FMT_SMF.1/EAC1PP	-	-	X	-	-	X
FMT_LIM.1/EAC1PP	-	-	-	-	-	X
FMT_LIM.2/EAC1PP	-	-	-	-	-	X
FMT_MTD.1/INI_ENA_EAC1PP	-	-	-	-	-	X
FMT_MTD.1/INI_DIS_EAC1PP	-	-	-	-	-	X
FMT_MTD.1/CVCA_INI_EAC1PP	X	X	X	-	-	-
FMT_MTD.1/CVCA_UPD_EAC1PP	X	X	X	-	-	-
FMT_MTD.1/DATE_EAC1PP	X	X	X	-	-	-
FMT_MTD.1/CAPK_EAC1PP	X	X	X	-	-	-

TOE SFR / Security Function	TSF.AccessControl	TSF.Authenticate	TSF.SecureManagement	TSF.CryptoKey	TSF.AppletParametersSign	TSF.Platform
FMT_MTD.1/PA_EAC1PP	X	X	X	-	-	-
FMT_MTD.1/KEY_READ_EAC1PP	X	-	X	-	-	-
FMT_MTD.3/EAC1PP	-	X	-	-	-	-
FMT_LIM.1/Loader	-	-	-	-	-	X
FMT_LIM.2/Loader	-	-	-	-	-	X
FMT_MTD.1/AA_Private_Key	X	X	X	-	-	-
FPT_EMS.1/EAC2PP	-	-	-	-	-	X
FPT_FLS.1/EAC2PP	-	-	-	-	-	X
FPT_TST.1/EAC2PP	-	-	-	-	X	X
FPT_PHP.3/EAC2PP	-	-	-	-	-	X
FPT_TST.1/EAC1PP	-	-	-	-	X	X
FPT_FLS.1/EAC1PP	-	-	-	-	-	X
FPT_PHP.3/EAC1PP	-	-	-	-	-	X
FPT_EMS.1/EAC1PP	-	-	-	-	-	X
FPT_EMS.1/SSCDPP	-	-	-	-	-	X
FPT_FLS.1/SSCDPP	-	-	-	-	-	X
FPT_PHP.1/SSCDPP	-	-	-	-	-	X
FPT_PHP.3/SSCDPP	-	-	-	-	-	X
FPT_TST.1/SSCDPP	-	-	-	-	X	X

3878 **7.4. Correspondence of SFR and TOE mechanisms**

3879 Each TOE security functional requirement is implemented by at least one TOE mechanism. In
 3880 section 7.1 the implementing of the TOE security functional requirement is described in form
 3881 of the TOE mechanism.

3882 **8. GLOSSARY AND ABBREVIATIONS**

3883 For Glossary and Acronyms please refer to the corresponding section of [20].

3884 **9. BIBLIOGRAPHY**

- [1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- [2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- [3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
- [4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB- 2017-04-004, Version 3.1, Revision 5, April 2017
- [5] BSI: Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012 v1.3.2 (5. December 2012)
- [6] BSI: Common Criteria Protection Profile - ID-Card implementing Extended Access Control 2 as defined in BSI TR-03110, BSI-CC-PP-0086-2015 v1.01 (May 20th, 2015)
- [7] ICAO: Technical Report: Supplemental Access Control for Machine Readable Travel Documents, Version - 1.1, 15. April 2014.
- [8] ICAO: ICAO Doc 9303, Part 1: Machine Readable Passports, Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability, Seventh Edition, 2015
- [9] ICAO: ICAO Doc 9303 - Machine Readable Travel Documents, 7th edition, 2015
- [10] Inside Secure, Infineon Technologies AG, NXP Semiconductors Germany GmbH, STMicroelectronics: Common Criteria Protection Profile - Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, v1.0 (13.01.2014)
- [11] ISO/IEC 14443 Identification cards — Contactless integrated circuit cards,
- [12] ISO/IEC 7816-4:2013 Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange,
- [13] BSI: Common Criteria Protection Profile - Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01, v0.01, 22 July 2014
- [14] EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation
- [15] EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application

- [16] BSI: TR-03110-1 - Advanced Security Mechanisms for Machine Readable Travel Documents. Part 1 - eMRTDs with BAC/PACEv2 and EACv1, v2.20 (26. February 2015)
- [17] BSI: TR-03110-2 - Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token. Part 2 – Protocols for electronic IDentification, Authentication and trust Services (eIDAS) Version 2.21, 21. December 2016
- [18] BSI: TR-03110-3 - Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token. Part 3 - Common Specifications v2.21 (21. December 2016)
- [19] BSI: TR-03110-4 - Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token. Part 4 – Applications and Document Profiles V2.21, 21. December 2016
- [20] BSI: Common Criteria Protection Profile - Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP], BSI-CC-PP-0087 version 1.01, May 20th, 2015
- [21] IDentity Applet Suite v3.4 Administrator's Guide v3.4.1 (July 2020)
- [22] IDentity Applet Suite v3.4 User's Guide v3.4.5 (October 2022)
- [23] JCOP 4 P71 Security Target Lite, Security Target for JCOP 4 P71/SE050 Rev. 4.8 — 8 August 2022
- [24] JCOP 4 P71, User manual for JCOP 4 P71, Rev. 4.2, DocNo 469542, 05 August, 2022, NXP Semiconductors
- [25] Supporting Document Mandatory Technical Document Composite product evaluation for Smart Cards and similar devices; Version 1.5.1, May 2018
- [26] BSI: TR 03111: Elliptic Curve Cryptography, Version 2.0, 28. June 2012.
- [27] RSA Laboratories: PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
- [28] National Institute of Standards and Technology: FIPS PUB 180-4: Secure hash standard, March 2012.
- [29] Published by Oracle. Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., May 2015.
- [30] European card for e-Services and National e-ID applications, IAS ECC European Citizen Card, Technical Specifications, Revisions 1.0.1.
- [31] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie - Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 09. Januar 2013, BSI-TR02102.

- [32] Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication, version 1.0, March 8,2016, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan
- [33] Protection Profile for ePassport IC with SAC (PACE) and Active Authentication, version 1.0, March 8,2016, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan
- [34] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) Security Target Lite, Rev. 2.6, 13 June 2022
- [35] Certification Report - NXP Secure Smart Card Controller N7121 with IC NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) BSI-DSZ-CC-1136-V3-2022