



# **Security Target Lite**

## **IDeal Citiz v2.3-n embedding ID.me 1.6-n application**

Reference: 2019\_2000043199

Issue Date: 2019-06-20

## DOCUMENT EVOLUTION

Version	Date	Author	Revision
1.0	20/06/2019	IDEMIA	Initial version based on the full security target (Reference: 2018_2000034214, Version: 4.0)

© IDEMIA. All rights reserved.

Specifications and information are subject to change without notice.

The products described in this document are subject to continuous development and improvement.

All trademarks and service marks referred to herein, whether registered or not in specific countries, are the properties of their respective owners.

*- Printed versions of this document are uncontrolled -*

## Table of contents

<b>1</b>	<b>TOE OVERVIEW.....</b>	<b>7</b>
1.1	ST IDENTIFICATION .....	8
1.2	TOE REFERENCE.....	8
1.3	TOE DOCUMENTATION .....	8
<b>2</b>	<b>TECHNICAL TERMS, ABBREVIATION AND ASSOCIATED REFERENCES.....</b>	<b>9</b>
2.1	TECHNICAL TERMS .....	9
2.2	ABBREVIATION.....	14
2.3	ASSOCIATED REFERENCES .....	16
<b>3</b>	<b>TOE DESCRIPTION .....</b>	<b>18</b>
3.1	PRODUCT PRESENTATION .....	18
3.2	TOE TYPE.....	18
3.3	TOE FUNCTIONS.....	20
3.4	OPERATION OF THE TOE.....	21
3.5	MAJOR SECURITY FEATURES OF THE TOE .....	26
3.5.1	<i>Authentication mechanisms .....</i>	<i>26</i>
3.5.2	<i>Cryptographic operations.....</i>	<i>26</i>
3.5.3	<i>Trusted Channel function.....</i>	<i>26</i>
3.5.4	<i>Access Control function .....</i>	<i>26</i>
3.5.5	<i>Data Storage function .....</i>	<i>26</i>
3.5.6	<i>Integrity function .....</i>	<i>26</i>
3.5.7	<i>Features from the Platform.....</i>	<i>27</i>
<b>4</b>	<b>TOE LIFE CYCLE .....</b>	<b>28</b>
4.1	GENERAL.....	28
4.2	DEVELOPMENT PHASE .....	29
4.3	PRODUCTION PHASE.....	29
4.4	PREPARATION PHASE .....	31
4.5	OPERATIONAL PHASE.....	31
<b>5</b>	<b>CONFORMANCE CLAIMS.....</b>	<b>32</b>
5.1	CC CONFORMANCE .....	32
5.2	PP CLAIMS .....	32
5.3	CONFORMANCE RATIONALE .....	33
<b>6</b>	<b>SECURITY PROBLEM DEFINITION .....</b>	<b>40</b>
6.1	ASSETS.....	40
6.1.1	<i>Primary Assets .....</i>	<i>40</i>
6.1.2	<i>Primary Assets related to EAC2 .....</i>	<i>40</i>
6.1.3	<i>Secondary Assets related to EAC2 .....</i>	<i>41</i>
6.2	USERS / SUBJECTS.....	42
6.2.1	<i>Users/Subjects related to EAC2 .....</i>	<i>42</i>
6.2.2	<i>Threat agents .....</i>	<i>44</i>
6.2.3	<i>Miscellaneous .....</i>	<i>44</i>
6.3	THREATS.....	44
6.3.1	<i>Threats related to EAC2.....</i>	<i>44</i>
6.3.2	<i>Miscellaneous .....</i>	<i>46</i>
6.4	ORGANISATIONAL SECURITY POLICIES .....	47
6.4.1	<i>OSP related to EAC2.....</i>	<i>47</i>
6.4.2	<i>Miscellaneous .....</i>	<i>49</i>
6.5	ASSUMPTIONS .....	50
6.5.1	<i>All SSCD parts.....</i>	<i>50</i>
6.5.2	<i>Parts 3 and 6 only.....</i>	<i>50</i>

<b>7</b>	<b>SECURITY OBJECTIVES .....</b>	<b>51</b>
7.1	SECURITY OBJECTIVES FOR THE TOE .....	51
7.1.1	<i>All SSCD parts.....</i>	<i>51</i>
7.1.2	<i>SSCD parts 2, 4 and 5 only.....</i>	<i>52</i>
7.1.3	<i>SSCD parts 3 and 6 only.....</i>	<i>52</i>
7.1.4	<i>SSCD part 4 only.....</i>	<i>53</i>
7.1.5	<i>SSCD parts 5 and 6 only.....</i>	<i>53</i>
7.1.6	<i>Security Objectives OT related to EAC2 .....</i>	<i>53</i>
7.2	SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT .....	56
7.2.1	<i>All SSCD parts.....</i>	<i>56</i>
7.2.2	<i>SSCD parts 3 and 6 only.....</i>	<i>57</i>
7.2.3	<i>SSCD part 4 only.....</i>	<i>58</i>
7.2.4	<i>SSCD parts 5 and 6 only.....</i>	<i>58</i>
7.2.5	<i>Security Objectives OE related to EAC2 .....</i>	<i>59</i>
7.3	SECURITY OBJECTIVES RATIONALE.....	61
7.3.1	<i>Threats .....</i>	<i>61</i>
7.3.2	<i>Organisational Security Policies .....</i>	<i>64</i>
7.3.3	<i>Assumptions .....</i>	<i>68</i>
7.3.4	<i>SPD and Security Objectives .....</i>	<i>68</i>
<b>8</b>	<b>EXTENDED REQUIREMENTS .....</b>	<b>75</b>
8.1	EXTENDED FAMILY FPT_EMS - TOE EMANATION .....	75
8.2	EXTENDED FAMILY FIA_API - AUTHENTICATION PROOF OF IDENTITY .....	76
8.3	EXTENDED FAMILY FCS_RND - GENERATION OF RANDOM NUMBERS .....	77
8.4	EXTENDED FAMILY FMT_LIM - LIMITED CAPABILITIES .....	78
<b>9</b>	<b>SECURITY REQUIREMENTS .....</b>	<b>80</b>
9.1	SECURITY FUNCTIONAL REQUIREMENTS .....	80
9.1.1	<i>All SSCD parts.....</i>	<i>80</i>
9.1.2	<i>SSCD parts 2, 4 and 5 only.....</i>	<i>89</i>
9.1.3	<i>SSCD parts 3 and 6 only.....</i>	<i>91</i>
9.1.4	<i>SSCD part 4 only.....</i>	<i>93</i>
9.1.5	<i>SSCD parts 5 and 6 only.....</i>	<i>94</i>
9.1.6	<i>Additional SFRs related to EAC2 .....</i>	<i>95</i>
9.2	SECURITY ASSURANCE REQUIREMENTS.....	105
9.3	SECURITY REQUIREMENTS RATIONALE .....	106
9.3.1	<i>Objectives .....</i>	<i>106</i>
9.3.2	<i>Rationale tables of Security Objectives and SFRs.....</i>	<i>113</i>
9.3.3	<i>Dependencies .....</i>	<i>120</i>
9.3.4	<i>Rationale for the Security Assurance Requirements .....</i>	<i>126</i>
<b>10</b>	<b>TOE SUMMARY SPECIFICATION.....</b>	<b>127</b>
10.1	TOE SUMMARY SPECIFICATION.....	127
10.1.1	<i>Chip security functionalities .....</i>	<i>127</i>
10.1.2	<i>Platform security functionalities.....</i>	<i>127</i>
10.1.3	<i>Application security functionalities.....</i>	<i>127</i>
10.2	SFRs AND TSS.....	132
10.2.1	<i>SFRs and TSS - Rationale .....</i>	<i>132</i>

## Table of figures

Figure 1: TOE physical scope .....19

Figure 2: TOE and operational environments with Key Generation .....22

Figure 3: TOE and operational environments with Key Import .....22

Figure 4: TOE and operational environments with Key Generation and trusted channel to CGA .....23

Figure 5: TOE and Operational environments with Key Generation and trusted channel to SCA .....23

Figure 6: TOE and Operational environments with Key Import and trusted channel to SCA .....24

Figure 7: Scope of the SSCD .....25

Figure 8: TOE Life Cycle .....28

## Table of tables

Table 1	PP SPDs vs. ST.....	35
Table 2	PP Security Objectives vs. ST .....	37
Table 3	PP SFRs vs. ST .....	39
Table 4	Threats and Security Objectives - Coverage .....	69
Table 5	Security Objectives and Threats - Coverage .....	70
Table 6	OSPs and Security Objectives - Coverage.....	71
Table 7	Security Objectives and OSPs - Coverage.....	73
Table 8	Assumptions and Security Objectives for the Operational Environment - Coverage .....	73
Table 9	Security Objectives for the Operational Environment and Assumptions - Coverage .....	74
Table 10	Security Objectives and SFRs - Coverage .....	116
Table 11	SFRs and Security Objectives .....	120
Table 12	SFRs Dependencies .....	124
Table 13	SARs Dependencies .....	125

# 1 TOE Overview

---

This document is the Security Target Lite for the IDEal Citiz v2.3-n embedding ID.me 1.6-n which is a IDEMIA specific Java Card implementation of the Identification Authentication Signature for European Citizen Card v1.0.1 [IAS ECC].

ID.me 1.6-n is designed to be compliant with the IAS ECC v1.0.1 specification [IAS ECC], taking into account the addendum [IAS ADD].

The TOE addressed by the current ST is a SSCD device according to European Regulation 910/2014 [EU-REG-910/2014] and implementing act [EU-IMP-2016-650] with functionality covered in (a combination of) the following SSCD protection profiles:

- 1) SSCD Part 2: that performs the generation of signature keys in the device [PP-SSCD2],
- 2) SSCD Part 3: that performs the import of the signature keys generated in a trusted manner outside the device [PP-SSCD3],
- 3) SSCD Part 4: that specifies an extension for an SSCD with key generation (SSCD Part 2) that support establishing a trusted channel with a certificate generation application (CGA) [PP-SSCD4],
- 4) SSCD Part 5: that specifies an extension for an SSCD with key generation (SSCD Part 2) that additionally supports establishing a trusted channel with a signature creation application (SCA) ) [PP-SSCD5] and
- 5) SSCD Part 6: that specifies an extension for an SSCD with key import (SSCD Part 3) that additionally supports establishing a trusted channel with a signature creation application (SCA) [PP-SSCD6].
- 6) The TOE adds EAC V2 protocol. The additional functions of the protocol are based on the PP EACV2 defined in [EAC2-PP].

ID.me 1.6-n Application is a set of Java card services intended to be used exclusively on the NXP JCOP 3 P60 open platform, which is certified according to CC EAL 5+ [ST-PL]. This platform is based on the NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software (Certification ID: BSI-DSZ-CC-1059-2018) and Crypto Library V3.1.2 on P6022y VB (Certification ID: CC-18-67206).

This ST has been conceived to prepare a Common Criteria evaluation following the “compositional approach” described in [COMP]. This approach consists in starting from a Platform that has been independently certified, and performing an evaluation of the composite product resulting from embedding an Application into it, using some of the results from the evaluation of the NXP JCOP 3 P60 open platform certified by the Dutch NSCIB certification body (CC-18-98209/2).

This Security Target describes:

- The Target of Evaluation (TOE)
- The assets to be protected, the threats (T) to be countered by the TOE itself during the usage of the TOE,
- The organizational security policies (OSP), and the assumptions (A),
- The security objectives (OT) for the TOE and its environment (OE),
- The security functional requirements (SFR) for the TOE and its IT environment,
- The TOE security assurance requirements (SAR),
- The TOE Summary specification (TSS).

## 1.1 ST Identification

<b>Title</b>	Security Target IDEal Citiz v2.3-n embedding ID.me 1.6-n application
<b>Reference</b>	2019_2000043199
<b>Version</b>	1.0
<b>ITSEF</b>	CEA-LETI
<b>Certification Body</b>	ANSSI
<b>Author</b>	IDEMIA
<b>CC Version</b>	3.1 Revision 5
<b>Assurance Level</b>	EAL5 augmented with ALC_DVS.2 and AVA_VAN.5
<b>Protection Profiles</b>	PP SSCD-Part 2 Key Generation [PP-SSCD2], PP SSCD-Part 3 Key Import [PP-SSCD3], PP SSCD-Part 4 Key Generation and Trusted Channel with CGA [PP-SSCD4] PP SSCD-Part 5 Key Generation and Trusted Channel with SCA [PP-SSCD5] PP SSCD-Part 6 Key Import and Trusted Channel with SCA [PP-SSCD6]

## 1.2 TOE Reference

<b>TOE name</b>	IDEal Citiz v2.3-n embedding ID.me 1.6-n application
<b>Applet identification</b>	ID.me 1.6-n / 2.1.6.0.0
<b>Platform name</b>	NXP JCOP 3 P60 certified by the Dutch NSCIB certification body (CC-18-98209/2) on 29-11-2018
<b>Platform identification</b>	Platform ID: "JxHyyy0019790400" (SVN 6521; "OSB RC9") Patch ID: 00 00 00 00 00 00 00 00 (no patch) 04 00 00 00 00 00 00 00 (PL4)
<b>IC reference</b>	NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software certified by the German certification body (BSI-DSZ-CC-1059-2018) on 18-05-2018
<b>Crypto Lib reference</b>	Crypto Library V3.1.2 on P6022y VB certified by the Dutch NSCIB certification body (CC-18-67206) on 31-05-2018

## 1.3 TOE documentation

TOE documentation is described in the table below:

Reference	Description
<a href="#">[AGD_PRE]</a>	2018_2000033006 - AGD_PRE - IDEalCitiz v2.3-n - Preparative Procedures, v2.3
	2018_2000033005 - AGD_PRE - IDEalCitiz v2.3-n - Personalization Specification, v2.2
<a href="#">[AGD_OPE]</a>	2018_2000033003 - AGD_OPE - IDEalCitiz v2.3-n - Operational Guidance, v2.2
	2018_2000033004 - AGD_OPE - IDEalCitiz v2.3-n - User Manual, v2.2



## 2 Technical terms, Abbreviation and Associated references

### 2.1 Technical terms

Term	Definition
<b>Application note</b>	<i>Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.</i>
<b>Administrator</b>	<i>user who performs TOE initialization, TOE personalization, or other TOE administrative functions</i>
<b>Advanced electronic signature</b>	<i>An electronic signature which meets the following requirements [DIR]:</i> <ul style="list-style-type: none"> <li><i>(i) it is uniquely linked to the signatory,</i></li> <li><i>(ii) it is capable of identifying the signatory,</i></li> <li><i>(iii) it is created using means that the signatory can maintain under his sole control,</i></li> <li><i>(iv) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.</i></li> </ul>
<b>Authentication data</b>	<i>information used to verify the claimed identity of a user</i>
<b>Authentication</b>	<i>Authentication defines a procedure that verifies the identity of the communication partner. The most elegant method is based on the use of so called digital signatures.</i>

<b>Card Access Number (CAN)</b>	<i>A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the Identification Card), semi-static (e.g. printed on a label on the Identification Card) or dynamic (randomly chosen by the Card and displayed by it using e.g. ePaper, OLED or similar technologies)</i>
<b>Certificate</b>	<i>digital signature used as electronic attestation binding signature-verification data to a person confirming the identity of that person as legitimate signer</i>
<b>Certificate info</b>	<p><i>information associated with an SCD/SVD pair that may be stored in a secure signature creation device</i></p> <p><i>NOTE 1: Certificate info is either</i></p> <ul style="list-style-type: none"> <li>- <i>a signer's public key certificate or,</i></li> <li>- <i>one or more hash values of a signer's public key certificate together with an identifier of the hash function used to compute the hash values.</i></li> </ul> <p><i>NOTE 2: Certificate info may contain information to allow the user to distinguish between several certificates.</i></p>
<b>Certificate-generation application (CGA)</b>	<i>collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate</i>
<b>Certificate revocation list</b>	<i>A list of revoked certificates issued by a certificate authority</i>
<b>Certification service provider (CSP)</b>	<i>entity that issues certificates or provides other services related to electronic signatures</i>
<b>Data to be signed (DTBS)</b>	<i>all of the electronic data to be signed including a user message and signature attributes</i>
<b>Data to be signed or its unique representation (DTBS/R)</b>	<p><i>data received by a secure signature creation device as input in a single signature creation operation</i></p> <p><i>NOTE: Examples of DTBS/R are</i></p> <ul style="list-style-type: none"> <li>- <i>a hash value of the data to be signed (DTBS), or</i></li> <li>- <i>an intermediate hash value of a first part of the DTBS complemented with a remaining part of the DTBS, or</i></li> <li>- <i>the DTBS.</i></li> </ul>
<b>ECC</b>	<i>(Elliptic Curve Cryptography) class of procedures providing an attractive alternative for the probably most popular asymmetric procedure, the RSA algorithm.</i>
<b>Hash function</b>	<i>A function which forms the fixed-size result (the hash value) from an arbitrary amount of data (which is the input). These functions are used to generate the electronic equivalent of a fingerprint. The significant factor is that it must be impossible to generate two entries which lead to the same hash value (so called collisions) or even to generate a matching message for a defined hash value.</i>

<b>Integrity</b>	<i>The test on the integrity of data is carried out by checking messages for changes during the transmission by the receiver. Common test procedures employ Hash functions, MACs (Message Authentication Codes) or – with additional functionality – digital signatures.</i>
<b>Javacard</b>	<i>A smart card with a Javacard operation system.</i>
<b>Legitimate user</b>	<i>An user of a secure signature creation device who gains possession of it from an SSCD provisioning service provider and who may be authenticated by the SSCD as its signatory.</i>
<b>MAC</b>	<i>Message Authentication Code. Algorithm that expands the message by means of a secret key by special redundant pieces of information, which are stored or transmitted together with the message. To prevent an attacker from targeted modification of the attached redundancy requires its protection in a suitable way.</i>
<b>Notified body</b>	<i>An organizational entity designated by a member state of the European Union as responsible for accreditation and supervision of the evaluation process for products conforming to [PP-SSCD2], [PP-SSCD5] and for determining admissible algorithms and algorithm parameters.</i>
<b>Non repudiation</b>	<i>One of the objectives in the employment of digital signatures. It describes the fact that the sender of a message is prevented from denying the preparation of the message. The problem cannot be simply solved with cryptographic routines, but the entire environment needs to be considered and respective framework conditions need to be provided by pertinent laws.</i>
<b>PACE Terminal (PCT)</b>	<i>A technical system verifying correspondence between the stored password and the related value presented to the terminal. PCT implements the terminal's part of the PACE protocol and authenticates itself to the Card using a shared password (CAN, PIN or PUK). The PCT is not allowed reading User Data.</i>
<b>Password Authenticated Connection Establishment (PACE)</b>	<i>The PACE Protocol is a password authenticated DiffieHellman key agreement protocol providing implicit password based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password <math>\eta</math>). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.</i>
<b>Private key</b>	<i>Secret key only known to the receiver of a message, which is used in asymmetric ciphers for encryption or generation of digital signatures.</i>
<b>Pseudo random number</b>	<i>Many cryptographic mechanisms require random numbers (e.g. in key generation). The problem, however, is that it is difficult to implement true random numbers in software. Therefore, so called pseudo random number generators are used, which then should be initialized with a real random element (the so called seed).</i>
<b>Public Key</b>	<i>Publicly known key in an asymmetric cipher which is used for encryption and verification of digital signatures.</i>
<b>Public key infrastructure (PKI)</b>	<i>Combination of hardware and software components, policies, and different procedures used to manage digital certificates.</i>
<b>Qualified certificate</b>	<i>public key certificate that meets the requirements laid down in Annex I and that is provided by a CSP that fulfils the requirements laid down in Annex II (the directive: 2.10) [DIR]</i>

<b>Qualified electronic signature</b>	<i>advanced electronic signature that has been created with an SSCD with a key certified with a qualified certificate ([DIR]: 5.1).</i>
<b>Random numbers</b>	<i>Many cryptographic algorithms or protocols require a random element, mostly in form of a random number, which is newly generated in each case. In these cases, the security of the procedure depends in part on the suitability of these random numbers. As the generation of real random numbers within computers still imposes a problem (a source for real random events can in fact only be gained by exact observation of physical events, which is not easy to realize for software), so called pseudo random numbers are used instead.</i>
<b>Reference authentication data (RAD)</b>	<i>Data persistently stored by the TOE for authentication of a user as authorised for a particular role.</i>
<b>Secure messaging</b>	<i>Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.</i>
<b>Secure signature creation device (SSCD)</b>	<i>Personalized device that meets the requirements laid down in [DIR], Annex III by being evaluated according to a security target conforming to this PP ([DIR]: 2.5 and 2.6).</i>
<b>Signatory</b>	<i>legitimate user of an SSCD associated with it in the certificate of the signature-verification data and who is authorized by the SSCD to operate the signature-creation function</i>
<b>Signature attributes</b>	<i>Additional information that is signed together with a user message.</i>
<b>Signature creation application (SCA)</b>	<i>Application complementing an SSCD with a user interface with the purpose to create an electronic signature. Note: A signature creation application is software consisting of a collection of application components configured to:</i> <ul style="list-style-type: none"> <li>▪ <i>present the data to be signed (DTBS) for review by the signatory,</i></li> <li>▪ <i>obtain prior to the signature process a decision by the signatory,</i></li> <li>▪ <i>if the signatory indicates by specific unambiguous input or action its in-tent to sign send a DTBS/R to the TOE,</i></li> <li>▪ <i>process the electronic signature generated by the SSCD as appropriate, e.g. as attachment to the DTBS.</i></li> </ul>
<b>Signature creation data (SCD)</b>	<i>private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature</i>
<b>Signature creation system (SCS)</b>	<i>complete system that creates an electronic signature consisting of an SCA and an SSCD</i>
<b>Signature verification data (SVD)</b>	<i>public cryptographic key that can be used to verify an electronic signature</i>
<b>Signed data object</b>	<i>The electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.</i>

<b>Smart card</b>	<i>A smart card is a chip card which contains an internal micro controller with CPU, volatile (RAM) and non-volatile (FLASH) memory, i.e. which can carry out its own calculations in contrast to a simple storage card. Sometimes a smart card has a numerical coprocessor (NPU) to execute public key algorithms efficiently. Smart cards have all of their functionality comprised on a single chip (in contrast to chip cards, which contain several chips wired to each other). There-fore, such a smart card is ideal for use in cryptography as it is almost impossible to manipulate its internal processes.</i>
<b>SSCD provisioning service</b>	<i>service to prepare and provide an SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD</i>
<b>User</b>	<i>entity (human user or external IT entity) outside the TOE that interacts with the TOE</i>
<b>User Message</b>	<i>data determined by the signatory as the correct input for signing</i>
<b>Verification authentication data (VAD)</b>	<i>data provided as input to a secure signature creation device for authentication by cognition or by data derived from a user's biometric characteristics</i>

## 2.2 Abbreviation

<b>Acronym</b>	<b>Definition</b>
<b>ADF</b>	<i>Application Dedicated File</i>
<b>CA</b>	<i>Certification authority</i>
<b>CAD</b>	<i>card acceptance device</i>
<b>CAN</b>	<i>Card Access Number</i>
<b>CC</b>	<i>Common Criteria</i>
<b>CGA</b>	<i>Certification generation application</i>
<b>CPU</b>	<i>Central Processing Unit</i>
<b>CSP</b>	<i>certification service provider</i>
<b>DPA</b>	<i>differential power analysis</i>
<b>DTBS</b>	<i>Data to be signed</i>
<b>DTBS/R</b>	<i>Data to be signed or its unique representation</i>
<b>EAL</b>	<i>Evaluation assurance level</i>
<b>ECC</b>	<i>Elliptic Curve Cryptography</i>
<b>EEPROM</b>	<i>electrically erasable programmable read only memory</i>
<b>HID</b>	<i>human interface device</i>
<b>IT</b>	<i>Information technology</i>
<b>MAC</b>	<i>Message Authentication Code</i>

<b>OSP</b>	<i>Organizational security policy</i>
<b>PACE</b>	<i>Password Authenticated Connection Establishment</i>
<b>PIN</b>	<i>Personal Identification Number</i>
<b>PP</b>	<i>Protection profile</i>
<b>PUK</b>	<i>PIN Unblocked Key</i>
<b>RAD</b>	<i>Reference authentication data</i>
<b>RAM</b>	<i>random access memory</i>
<b>RNG</b>	<i>random number generation</i>
<b>ROM</b>	<i>read only memory</i>
<b>SAR</b>	<i>Security Assurance Requirements</i>
<b>SCA</b>	<i>Signature creation application</i>
<b>SCD</b>	<i>Signature creation data</i>
<b>SCS</b>	<i>Signature creation system</i>
<b>SDO</b>	<i>Security data object</i>
<b>SF</b>	<i>security function</i>
<b>SFP</b>	<i>Security function policy</i>
<b>SFR</b>	<i>Security functional requirement</i>
<b>SPA</b>	<i>simple power analysis</i>
<b>SSCD</b>	<i>Secure signature creation device</i>
<b>ST</b>	<i>Security target</i>
<b>SVD</b>	<i>Signature verification data</i>
<b>TOE</b>	<i>Target of evaluation</i>
<b>TSF</b>	<i>TOE security functionality</i>
<b>VAD</b>	<i>Verification authentication data</i>

## 2.3 Associated references

<b>[AIS20]</b>	Bundesamt fuer Sicherheit in der Informationstechnik. Anwendungshinweise und Interpretationen zum Schema, AIS 20: Funktionalitaetsklassen und Evaluationsmethodologie fuer deterministische Zufallszahlengeneratoren, Version 2.1, 2.12.2011.
<b>[CC1]</b>	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017. CCMB-2017-04-001.
<b>[CC2]</b>	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-002.
<b>[CC3]</b>	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-003.
<b>[CEM]</b>	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 5. April 2017. CCMB-2017-04-004.
<b>[COMP]</b>	Composite product evaluation for smart cards and similar devices, Version 1.5.1, May 2018.
<b>[CR-IC]</b>	Certification report BSI-DSZ-CC-1059-2018 for NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software, 18 May 2018, v1.0
<b>[D14890-2]</b>	Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services.
<b>[DIR]</b>	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures.
<b>[EAC2-PP]</b>	Common Criteria Protection Profile Profile Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110, BSI-CC-PP-0086, Version 1.01, May 20th, 2015, BSI
<b>[EU-IMP-2016-650]</b>	COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
<b>[EU-REG-910/2014]</b>	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
<b>[GP]</b>	GlobalPlatform Card Specification 2.2.1, GPC_SPE_034, GlobalPlatform Inc., January 2011.
<b>[IAS ADD]</b>	0000098587-01 Addendum IAS-ECC v1.0.1UK.
<b>[IAS ECC]</b>	Identification Authentication Signature - European Citizen Card Technical Specifications Revision: 1.0.1.
<b>[ICAO9303]</b>	International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – 7th edition, 2015
<b>[JCAPI]</b>	Published by Oracle. Java Card 3 Platform, Application Programming Interface, Classic Edition, Version3.0.4. September 2011.
<b>[JCRE]</b>	Published by Oracle. Java Card 3 Platform, Runtime Environment Specification, Classic Edition, Version3.0.4, E18985-01., September 2011.



<b>[JCVM]</b>	Published by Oracle. Java Card 3 Platform, Virtual Machine Specification, Classic Edition, Version 3.0.4, E25256-01., September 2011.
<b>[PACEPP]</b>	Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE – Common Criteria Protection Profile, BSI-CC-PP-0068-V2-2011, Version 1.0, 2 <sup>nd</sup> November 2011.
<b>[PP-IC]</b>	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014.
<b>[PP-PL]</b>	JavaCard Protection Profile – Open Configuration, Version 3.0, May, 2012. Certified by ANSSI under the reference ANSSI-CC-PP-2010/03-M01
<b>[PP-SSCD2]</b>	Protection profiles for secure signature creation device — Part 2: Device with key Generation BSI-CC-PP-0059-2009-MA-01, Version 2.0.1, February 2012.
<b>[PP-SSCD3]</b>	Protection profiles for secure signature creation device – Part3: Device with key import BSI-CC-PP-0075-2012, Version 1.0.2, September 2012
<b>[PP-SSCD4]</b>	Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application BSI-CC-PP-0071-2012, Version 1.0.1, December 2012.
<b>[PP-SSCD5]</b>	Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application BSI-CC-PP-0072-2012, Version 1.0.1, December 2012.
<b>[PP-SSCD6]</b>	Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature-creation application BSI-CC-PP-0076-2013, Version 1.0.4, April 2013
<b>[ST-PL]</b>	JCOP 3 P60, Security Target Lite, Rev. 3.8, 2018-10-23. NXP.
<b>[ST-IC]</b>	NXP Secure Smart Card Controller P6022y VB, Security Target Lite, Rev. 2.1, 6 April 2018
<b>[TR03110-2]</b>	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
<b>[TR03110-3]</b>	BSI: TR-03110-3: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token. Part 3 - Common Specifications, Version 2.21, 21 December 2016
<b>[UGM-PL]</b>	JCOP 3 SECID P60 CS (OSB), User Guidance and Administration Manual, Rev. 3.1 - 2018-10-23. NXP

## 3 TOE Description

---

### 3.1 Product Presentation

The product ID.eal Citiz v2.3-n embedding ID.me 1.6-n application is an integrated circuit chip embedding:

- An Operating system providing:
  - Java Card interfaces, as specified in [JCAPI]
  - Extended interfaces for targeted applications needs
  - A card manager application compliant with the Global Platform v2.2.1 specifications [GP] standard.
- An ID.me application compliant with the IAS ECC v1.0.1 specification [IAS ECC] with extensions for Elliptic Curve support [IAS ADD], PACE and EAC2 in accordance with [TR-03110-2] and [TR-03110-3].

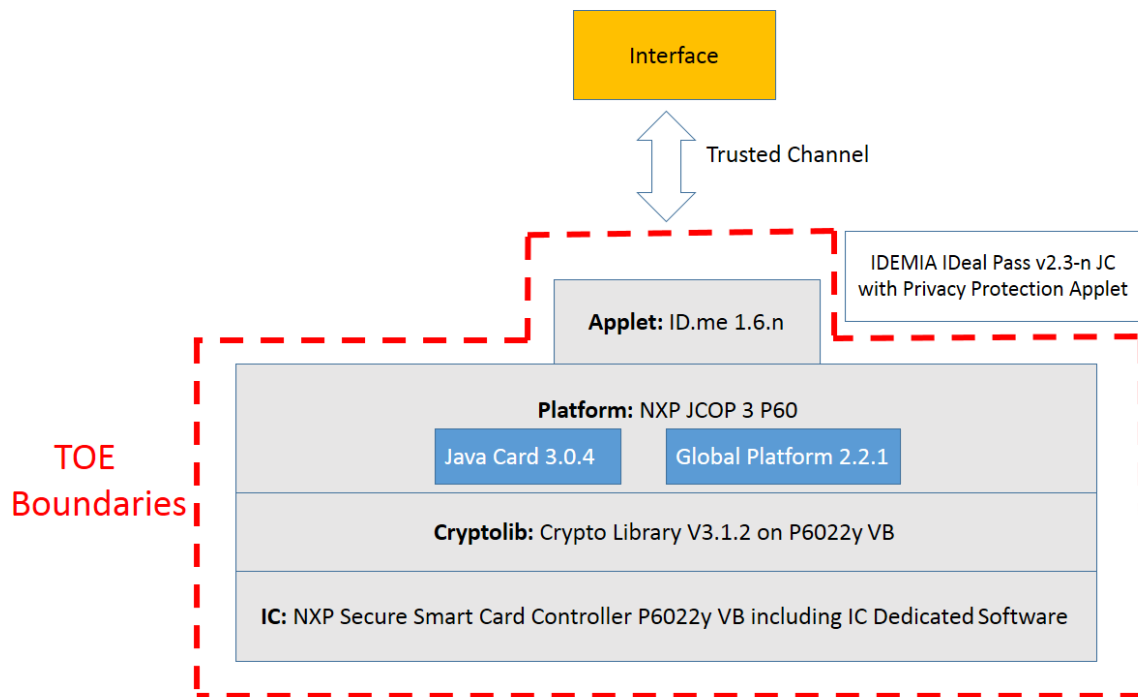
### 3.2 TOE Type

The ID.me is an European Card for e-Services and national e-ID Applications based on Java Card. ID.me is designed to be compliant with the IAS ECC v1.0.1 specification [IAS ECC], taking into account the addendum [IAS ADD]. It provides the following services:

- 1) SSCD containing data needed for generating electronic signatures on behalf of the Card Holder as well as for user authentication; this application is intended to be used in the context of official and commercial services, where an electronic signature of the Card Holder is required: to be certified according to [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6].
- 2) PACE authentication as defined in [TR-03110-2] to ensure a trusted channel for secure communication of the TOE with a SCA and a CGA.
- 3) Extended Access Control Version 2 (EAC2) as defined in [TR03110-2]. It consists of two parts: Chip Authentication Protocol Version 2 and Terminal Authentication Protocol Version 2.

The TOE comprises of

- The NXP P6022y VB including IC Dedicated Software with hardware for the contact and contactless interface,
- The Crypto Library V3.1.2 on P6022y VB,
- The NXP JCOP 3 P60 open platform,
- The applet containing SSCD and PKI functionalities (Optional) and,
- The associated guidance documentation [AGD\_OPE], [AGD\_PRE].



**Figure 1: TOE physical scope**

The ID.me Applet has been splitted into 3 modules. This permits to have ID.me configurations with and without PKI service and a better manageable amount of available memory in the TOE. The Applet contains the following three module configurations:

1. ID.me without PKI service
2. ID.me with PKI (IAS ECC) service
3. ID.me with PKI (EAC2) service

The PKI modules (IAS ECC and EAC2) implement mainly the following two additional functionalities:

- Asymmetric Role Auth mechanism on RSA as defined in IAS-ECC [IAS ECC] specifications:
  - READ BINARY,
  - MSE SET,
  - GET DATA K.ICC,
  - PSO VERIFY CERTIFICATE,
  - GET CHALLENGE,
  - EXTERNAL AUTHENTICATE.
- Additional combination of the use of Role Authentication and Device Authentication enabling the possibility to configure rights to different roles for a certain authentication protocol.

The scope of this TOE encompasses the three module configurations mentioned above. The desired module configuration is loaded into the TOE's non-volatile memory in either pre-personalisation or IC manufacturing phase.

Since the TOE claims compliancy to 419 211-2 till EN 419 211-6 (Signature Protection Profiles [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6]), the TOE can (depending on the desired card profile/issuer policy) be used in the following SSCD configurations:

- **SSCD Config#1** claiming compliancy to CEN/EN 419 211-2/3/4/5/6 ([PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6]).
- **SSCD Config#2** claiming compliancy to CEN/EN 419 211-2/3/4 ([PP-SSCD2], [PP-SSCD3], [PP-SSCD4]). This configuration does not support the trusted channel between the TOE and the SCA.
- **SSCD Config#3** claiming compliancy to CEN/EN 419 211-2/3 ([PP-SSCD2], [PP-SSCD3]). This configuration does not support the trusted channel between: (i) the TOE and the SCA; (ii) the TOE and the CGA.

Beside the TOE, the product can include application instances of the Common Criteria certified IDEMIA IDEal Pass v2.3-n JC with Privacy Protection applet (out of scope of this TOE). IDEal Citiz v2.3-n enforces separation of the data between the applets and associated packages imposing logical separation of data using the Java Card™ Firewall [JCRE].

### 3.3 TOE Functions

The TOE is a combination of hardware and software configured to securely create, import, use and manage signature creation data (SCD). The SSCD protects the SCD during its whole life-cycle and during the signature creation process initialted solely by its signatory.

The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature. The TOE provides the following functions:

- generation of the SCD and the correspondent SVD,
- importation of the SCD and, optionally, the correspondent signature verification data (SVD)
- export the SVD for certification through a trusted channel to the CGA,
- prove the identity as SSCD to external entities
- optionally, receive and store certificate info,
- switch the TOE from a non operational state to an operational state, and
- if in an operational state, create digital signatures for data with the following steps:
  - select an SCD if multiple are present in the SSCD,
  - receive DTBS or a unique representation thereof DTBS/R through a trusted channel with SCA.
  - authenticate the signatory and determine its intent to sign,
  - apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R
- identification and authentication of trusted users and applications,
- data storage and protection from modification or disclosures, as needed,
- secure exchange of sensitive data between the TOE and a trusted applications,
- secure exchange of sensitive data between the TOE and a trusted human interface device.

The TOE is prepared for the signatory's use by

- generating or importing at least one SCD/SVD pair, and
- personalizing for the signatory by storing in the TOE:
  - the signatory's reference authentication data (RAD)
  - optionally, certificate info for at least one SCD in the TOE.

After preparation or import the SCD shall be in a non-operational state. Upon receiving a TOE the signatory shall verify its non-operational state and change the SCD state to operational.

After preparation, the intended, legitimate user should be informed of the signatory's verification authentication data (VAD) required for enabling the TOE's SVD operation for signature creation. If the VAD is a password, PIN or a biometric template, providing this information shall protect the confidentiality of the corresponding RAD.

If the use of an SCD is no longer required, then it shall be destroyed (e.g. by erasing it from memory) as well as its associated certificates.

### 3.4 Operation of the TOE

This section presents a functional overview of the TOE in its distinct operational environments:

- 1) **The preparation environment**, where it interacts with a
  - a. certification service provider (CSP) through a SCD/SVD generation application to generate or import signature creation and validation data (SCD/SVD) and
  - b. certificate generation application (CGA) to obtain a certificate for the signature validation data (SVD) that corresponds with the SCD generator by the TOE or by the CSP.

In case of SCD/SVD generation by the CSP, the SCD/SVD generation application transmits the SVD to the CGA. Optionally, the TOE may export the SVD through a trusted channel allowing the CGA to check the authenticity of the SVD.

The preparation environment interacts further with the TOE to personalize it for the signatory with the initial value of the reference authentication data (RAD).

- 2) **The signing environment**, where it interacts with a signer through a signature creation application (SCA) to sign data after authenticating the signer as its signatory. The signature creation application provides the data to be signed (DTBS), or a unique representation thereof (DTBS/R) as input to the TOE signature creation function and obtains the resulting digital signature. Optionally, the TOE and the SCA may communicate through a trusted channel to ensure the confidentiality and the integrity of the DTBS/R.
- 3) **The management environments**, where it interacts with the user or an SSCD-provisioning service provider to perform management operations, e.g. for the signatory to reset a blocked RAD.

A single device, e.g. a smart card terminal, may provide the required secure environment for management and signing.

Figure 2 to Figure 6 shows the TOE, its operational environments and the interactions with the environment

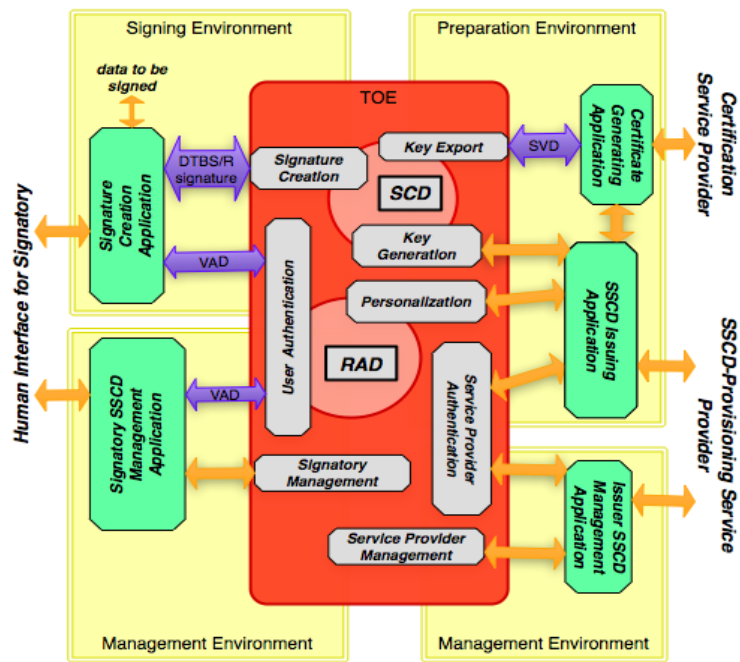


Figure 2: TOE and operational environments with Key Generation

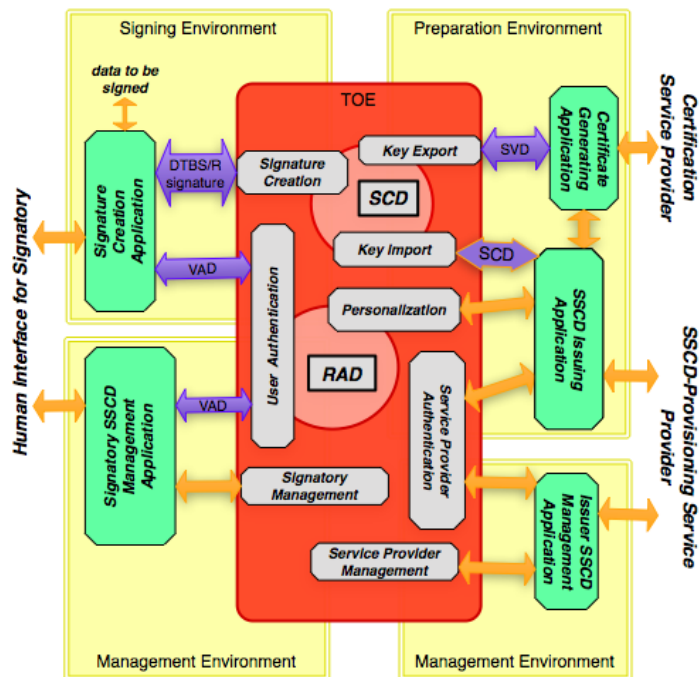


Figure 3: TOE and operational environments with Key Import

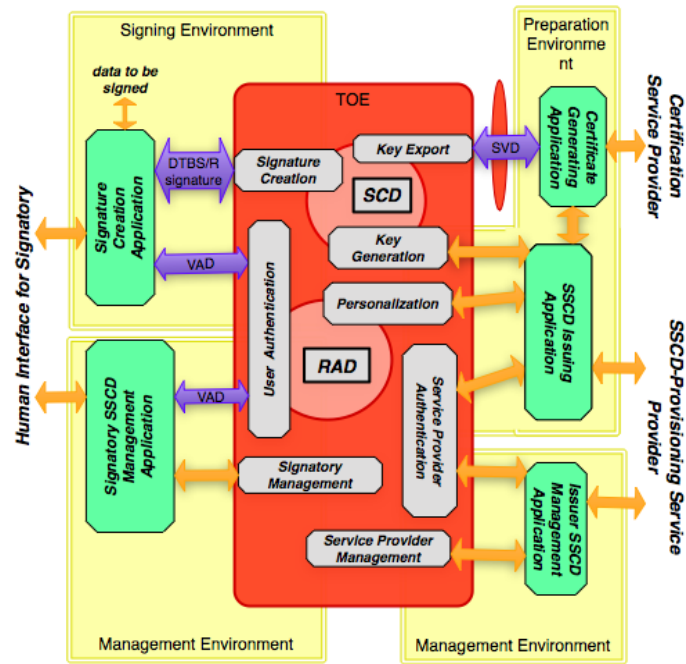


Figure 4: TOE and operational environments with Key Generation and trusted channel to CGA

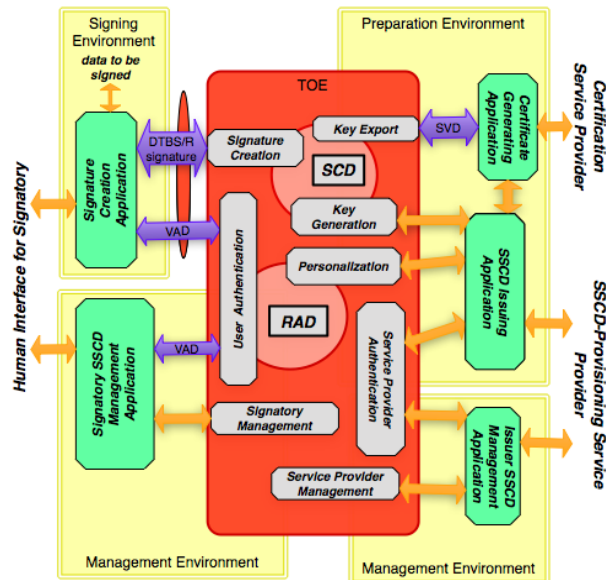
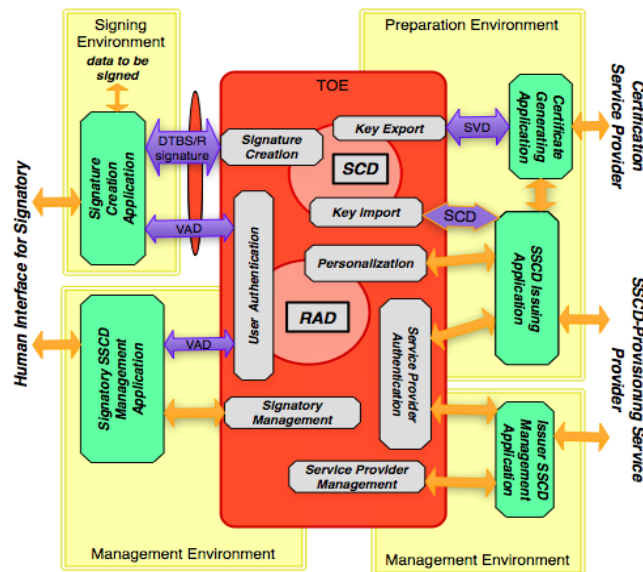


Figure 5: TOE and Operational environments with Key Generation and trusted channel to SCA





**Figure 6: TOE and Operational environments with Key Import and trusted channel to SCA**

The TOE stores signature creation data (SCD) and reference authentication data (RAD). The TOE may store multiple instances of SCD. In this case the TOE shall provide a function to identify each SCD and the SCA can provide an interface to the signer to select an SCD for use in the signature creation function of the SSSC. The TOE protects the confidentiality and integrity of the SCD and restricts its use in signature creation to its signatory. The digital signature created by the TOE is a qualified electronic signature as defined in Article 5.1 of the directive [DIR]. Determining the state of the certificate as qualified is beyond the scope of this standard.

The signature creation application shall protect the integrity of the input it provides to the TOE signature creation function as being consistent with the user data authorized for signing by the signatory. Unless implicitly known to the TOE, the SCA indicates the kind of the signing input (as DTBS/R) it provides and computes any hash values required. The TOE may augment the DTBS/R with signature parameters it stores and then computes a hash value over the input as needed by the kind of input and the used cryptographic algorithm. Optionally, the TOE and the SCA may communicate through a trusted channel in order to protect the integrity of the DTBS/R.

The TOE stores the signatory RAD to authenticate a user as its signatory. The RAD is a password e.g. PIN, a biometric template or a combination of these. The TOE protects the confidentiality and integrity of the RAD. The TOE receives the VAD from the signature creation application. The signature creation application protects the confidentiality of this data.

A certification service provider and a SSSC-provisioning service provider interact with the TOE in the secure preparation environment to perform any preparation function of the TOE required before control of the TOE is given to the legitimate user. These functions include but are not limited to:

- initializing the RAD,
- generating a key pair,
- storing personal information of the legitimate user.



Optionally, the TOE and the CGA communicate through a trusted channel in order to protect the integrity and authenticity of the SVD exported from the TOE.

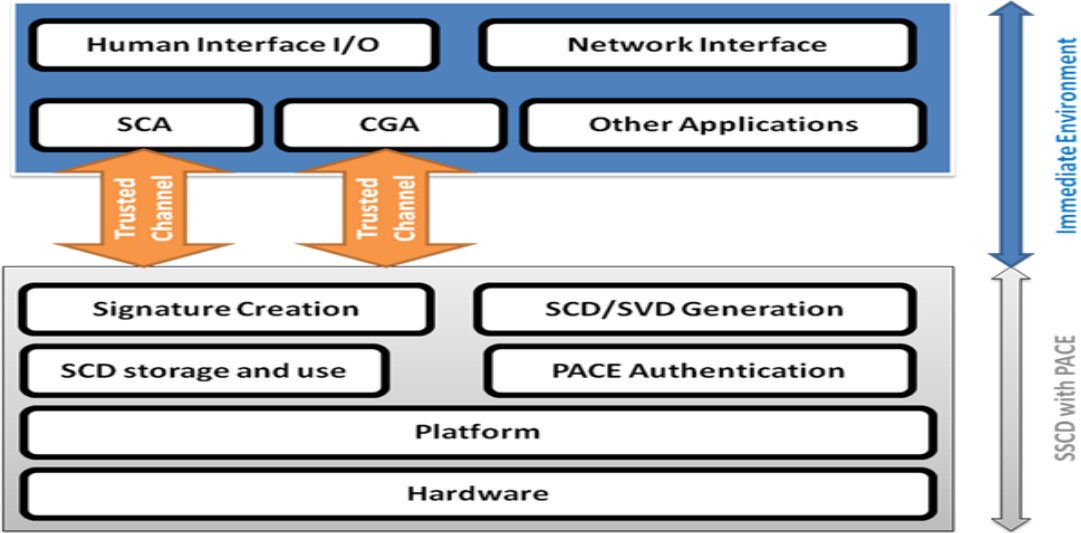
In case the TOE shall support communication over a contactless interface the PACE protocol with PIN, PUK passwords as specified in [TR-03110-2] shall be configured and enforced by the TOE in order to obtain an secure messaging channel.

A smart card terminal shall be deployed, that provides the required secure environment to handle a request for signatory authorization. A signature can be obtained on a document prepared by a signature creation application component running on personal computer connected to the card terminal. The signature creation application initiates the digital signature creation function of the smart card through the terminal, after presenting the document to the user and after obtaining the authorization.

This TOE does not implement, in addition to the functions of the SSCD, the signature creation application (SCA). The SCA presents the data to be signed (DTBS) to the signatory and prepares the DTBS representation the signatory wishes to sign before performing the cryptographic function of the signature. The SCA is considered to be part of the environment of the TOE.

- The TOE supports user authentication by
1. itself or by
  2. an external IT entity, like a trusted human interface device or service connected via a trusted channel with the TOE.

The human interface device is used for the input of VAD for authentication by knowledge or for the generation of VAD for authentication by biometric characteristics.



**Figure 7: Scope of the SSCD**

The security functionality of the TOE will be externally available to the user by APDU commands according to the access conditions specified by the appropriate policies considering the life cycle state, user role and security state.

## 3.5 Major security features of the TOE

The TOE provides the following TOE security features:

### 3.5.1 Authentication mechanisms

This feature realizes the following authentication mechanisms [IAS ECC]:

- PIN verification,
- biometric characteristic verification and alternatively authentication with the PACE protocol,
- External Role authentication mechanisms
- Device authentication mechanisms
- Personalizer Authentication during the Phase 6 of the life cycle
- Terminal Authentication Version 2
- Chip Authentication Version 2

It also ensures that only authenticated terminals can get access to the user data stored on the TOE.

### 3.5.2 Cryptographic operations

This feature performs high level cryptographic operations (key generation, Signature Creation, destruction of cryptographic keys and random number generation). The implementation is mainly based on the Security Functionalities provided by the platform.

### 3.5.3 Trusted Channel function

This feature realizes a secure communication channel to verify authenticity and integrity as well as securing confidentiality of user data between the TOE and other devices connected. The TOE provides:

- Secure messaging with external applications as CGA and SCA
- PACE used to establish session keys for secure messaging
- TDES for encryption/decryption and MAC generation/verification
- AES for encryption/decryption and MAC generation/verification
- Chip Authentication used to establish new session keys for secure messaging

This feature is provided by the platform and used for secure messaging.

### 3.5.4 Access Control function

This feature manages the access to objects (files, directories, data and secrets) stored in the ID.me file system. It ensures secure management of secrets such as cryptographic keys. Access control is enforced by the APDU methods as specified in the interface defined in the functional specification.

### 3.5.5 Data Storage function

This feature manages the storage of manufacturing data, pre-personalization data and personalization data. This covers also the secure storage of SCD/SVD and RAD.

### 3.5.6 Integrity function

This feature monitors the integrity of sensitive user data and the integrity of the DTBS/R.

### ***3.5.7 Features from the Platform***

This contains all security functionalities provided by the certified platform (IC and Java Card operation system):

- Protection against malfunctions that are caused by exposure to operating conditions that may cause a malfunction. This includes hardware resets and operation outside the specified norms.
- Protection against tampering and the stored assets can not be retrieved or altered by physical manipulation
- Protection against physical attack and perform self tests as described in [ST-PL].
- Security domains are supported by the Java Card platform.
- Cryptographic operations: Signature generation, signature creation and secure messaging.

## 4 TOE Life Cycle

### 4.1 General

The TOE life cycle in Figure 8 distinguishes stages for development, production, preparation and operational use. The development and production of the TOE are subjects of CC evaluation according to the assurance life cycle (ALC) class. The development and production phases end with the delivery of the TOE to a SSCD-provisioning service provider. The functional integrity of the TOE shall be protected in delivering it to a SSCD-provisioning service provider: before any delivery occurs, the TOE is secured with a Transport Key. The SSCD-provisioning service will be able to unlock the card with the Transport Key before the preparation phase.

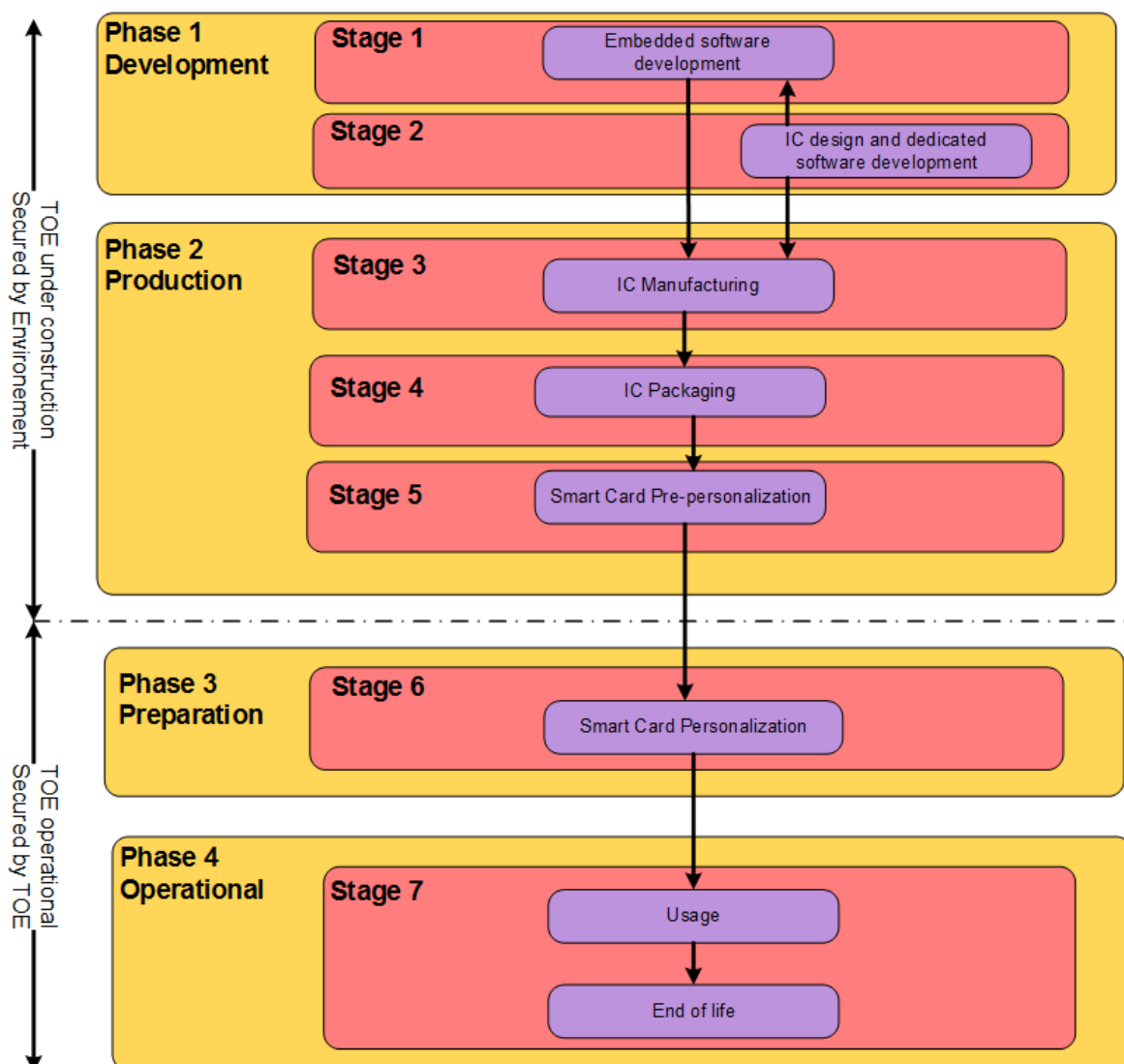


Figure 8: TOE Life Cycle

## 4.2 Development phase

This phase is composed of two stages:

- IC embedded software development (JCOP 3 platform and ID.me applet)
- IC development

The IC Developer designs the IC, develops the IC dedicated software and develops the guidance documentation associated with these TOE components.

The IC developer also acts as the developer of the operating system, which is the NXP JCOP 3 P60 open platform. The Platform Developer is responsible for:

- Specification, development and validation of the JCOP 3 platform.
- Use of the IC guidance documentation.

The Applet Developer is responsible for:

- Specification, development and validation of the ID.me applet.
- Use of the platform guidance documentation.

Roles, Actors, Sites and coverage for this phase of the product life-cycle are listed in the table below:

Role	Actor	Site	Covered by
ID.me Applet Developer	IDEMIA	Courbevoie, Noida and Haarlem R&D sites	ALC
Platform Developer	NXP	NXP development site(s) mentioned in CC platforme certificate	ALC
IC Developer	NXP	NXP development site(s) mentioned in CC IC certificate	ALC

## 4.3 Production phase

This phase is composed of three stages:

- IC manufacturing and testing
- IC Packaging
- Smartcard Prepersonalization & testing

At the end of Stage 1, some packages of ID.me applet are transferred to the chip manufacturer in order to be masked into the ROM.

Depending on the intention, the remaining packages for the desired ID.me module configurations (see section 3.2) can be either:

- (a) securely delivered directly from the Applet developer (IDEMIA R&D) to the IC manufacturer (NXP) in order to be loaded to EEPROM or
- (b) securely delivered directly from the Applet developer (IDEMIA R&D) to the Smartcard Pre-personalisation Agent (IDEMIA production sites) in order to be loaded to EEPROM.

The IC Manufacturer is responsible for producing the IC:

- IC manufacturing,
- Adding some packages of ID.me applet into the ROM,
- IC testing,

	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>30/142</b>
---	--	--

- Loading the remaining packages for the desired ID.me module configurations into the EEPROM (in case of alternative a),
- IC Initialization according to [UGM-PL].

The IC Packaging Manufacturer is responsible for IC packaging and testing.

The smart card pre-personalisation agent is responsible for loading the remaining packages for the desired ID.me module configurations into the EEPROM (in case of alternative b).

Roles, Actors, Sites and coverage for this phase of the product life-cycle are listed in the table below:

Role	Actor	Site	Covered by
IC Manufacturer	NXP	NXP production site(s) mentioned in [CR-IC]	ALC
IC Packaging Manufacturer	NXP or IDEMIA	NXP production site(s) mentioned in [CR-IC] or IDEMIA plant (Haarlem, Shenzhen, Vitré)	ALC
Smart Card Pre-personalisation agent	IDEMIA	IDEMIA plant (Haarlem, Shenzhen, Vitré)	ALC
<b>TOE Delivery Point</b>			

The following table describes the physical delivery of the TOE components from ALC phase to AGD phase:

TOE component	Identification	Package	Delivery method
IDEal Citiz v2.3-n embedding ID.me 1.6-n application	<b>Applet ID (Product name / Version):</b> ID.me 1.6-n / 2.1.6.0.0  <b>Platform ID:</b> JxHyyy0019790400  <b>Platform Patch ID:</b> 00 00 00 00 00 00 00 00 or 04 00 00 00 00 00 00 00	The package can be either of the following: - Chip modules contact-only, contactless or dual interface embedded in ID1 cards or any other (future) form factor, - Chip modules contact-only, contactless or dual interface on reel, - Contactless chip modules embedded in antenna inlays.	trusted courier
[AGD_PRE]	2018_2000033005, v2.2 2018_2000033006, v2.3	Electronic document	PGP-encrypted email
[AGD_OPE]	2018_2000033003, v2.2 2018_2000033004, v2.2	Electronic document	PGP-encrypted email
Personalization Agent Key set	n.a	Electronic file	PGP encrypted parts on USB or CD media, off-line registered distribution by trusted courier.

## 4.4 Preparation phase

All along this phase, the TOE is self-protected as it requires the authentication of the personalization agent prior to any operation. During this phase, creation of ID.me SSCD applet instance is mandatory.

This phase consists of:

- 1) SSCD ID.me applet instance creation of MF and one or more ADFs for the loaded module configuration according to [AGD\_PRE]:
  - a. ID.me SSCD without PKI service or
  - b. ID.me SSCD with PKI (IAS ECC) service or
  - c. ID.me SSCD with PKI (EAC2) service.
- 2) Personalisation according to [AGD\_PRE]:
  - a. RAD storage on SSCD
  - b. [OPTIONAL] Creation of SCD/SVD pair
    - i. by the TOE through the SCD/SVD generation functionality or
    - ii. by the Personalisation Agent, who loads the SCD and/or SVD into the TOE.
  - c. [OPTIONAL] export of SVD to CGA.
  - d. [OPTIONAL] storing back the obtained certificates
  - e. [OPTIONAL] depending on SSCD Config#1 or SSCD Config2#, required trusted channel cryptographic keys and mechanisms (e.g. PACE, EAC2, IAS-ECC CV certificates) for secure messaging with SCA and CGA.
- 3) Post-perso steps including: (i) ISD life-cycle management; (ii) disabling access to the Global Platform ISD (Card Manager) in order to prevent post issuance applet loading.

### *Application note:*

Personalisation steps 2b, 2c and 2d are not mandatory in preparation phase as they may be performed in operational phase of the TOE as well. Personalisation steps 2e is optional because it is not required for the SSCD Config#3.

## 4.5 Operational phase

The TOE is under the control of the User (Signatory and/or Administrator) and supports the functionality specified in [AGD\_OPE] and [UGM-PL].

## 5 Conformance Claims

---

### 5.1 CC Conformance

This Security Target claims conformance to the following documents defining the ISO/IEC 15408:2005 standard:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017. CCMB-2017-04-001.
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-002.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-003.
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision, April 2017. CCMB-2017-04-004.

Conformance to ISO/IEC 15408:2005 is claimed as follows:

- Part 1: conformant
- Part 2: extended with
  - FPT\_EMS.1 TOE Emanation [PP-SSCD2].
  - FCS\_RND Quality metric for random numbers [PACEPP].
  - FIA\_API Authentication proof of identity [PP-SSCD4].
  - FMT\_LIM - Limited capabilities [PACEPP].All the other security requirements have been drawn from the catalogue of requirements in [CC2].
- Part 3: conformant, compliant to EAL5 augmented with
  - ALC\_DVS.2 (Sufficiency of security measures)
  - AVA\_VAN.5 (Advanced methodical vulnerability analysis)

The TOE also includes:

- The NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software (Certification ID: BSI-DSZ-CC-0973-2016) and the Crypto Library V3.1.2 on P6022y VB (Certification ID: CC-16-67206-CR). The ST claims strict conformance to the security IC platform PP [PP-IC]. The assets, threats, objectives, SFR and security functions specific to IC and Crypto Library are not repeated in the current ST.
- The NXP JCOP 3 P60 open platform [ST-PL]. The ST claims demonstrable conformance to the security JC platform PP [PP-PL]. The assets, threats, objectives, SFR and security functions specific to the Platform are not repeated in the current ST.

### 5.2 PP Claims

This security target is compliant with the following PPs:

- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 2: Device with key generation" [PP-SSCD2].
- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 3: Device with key import" [PP-SSCD3].
- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 4: Extension for device with key generation and trusted communication with certificate generation application" [PP-SSCD4].



- “Common Criteria Protection Profile for Secure Signature Creation Device – Part 5: Extension for device with key generation and trusted communication with signature creation application” [PP-SSCD5].
- “Common Criteria Protection Profile for Secure Signature Creation Device – Part 6: Extension for device with key import and trusted communication with signature creation application” [PP-SSCD6].

### 5.3 Conformance Rationale

[PP-SSCD4] and [PP-SSCD5] are strictly conforming to the core PP-SSCD2 [PP-SSCD2]. [PP-SSCD6] is strictly conforming to the core PP-SSCD3 [PP-SSCD3]. This ST is claimed to be conformant to the above mentioned PPs [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6]. A detailed justification is given in the following:

- 1) The SPD of this ST contains the security problem definition [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6]. The SPD for this ST is described by the same threats, organisational security policies and assumptions as for the TOE in the PPs.
- 2) The security objectives for the TOE in this ST include all the security objectives for the TOE of the core PPs [PP-SSCD2] and [PP-SSCD3] and add
  - a. the security objectives OT.TOE\_TC\_VAD\_Imp and OT.TOE\_TC\_DTBS\_Imp from [PP-SSCD5] and [PP-SSCD6],
  - b. the security objectives OT.TOE\_SSCD\_Auth and OT.TOE\_TC\_SVD\_Exp from [PP-SSCD4],
- 3) The assumptions in this ST include A.CSP from [PP-SSCD3] and [PP-SSCD6]. This assumption doesn't mitigate any threat and doesn't fulfil any OSP meant to be addressed by security objectives for the TOE in the other PPs.
- 4) The security objectives for the operational environment in this ST include all security objectives for the operational environment of the core PPs [PP-SSCD2] and [PP-SSCD3] except OE.HI\_VAD, OE.DTBS\_Protect and OE.SSCD\_Prov\_Service.
  - This ST adapts OE.HI\_VAD and OE.DTBS\_Protect to the support provided by the TOE by new security functionality (cf. OT.TOE\_TC\_VAD\_Imp, OT.TOE\_TC\_DTBS\_Imp) provided by the TOE and changes them into OE.HID\_TC\_VAD\_Exp and OE.SCA\_TC\_DTBS\_Exp ([PP-SSCD5] and [PP-SSCD6] for details).
  - OE.SSCD\_Prov\_Service is replaced by OE.Dev\_Prov\_Service from [PP-SSCD4]. This ST also includes security objectives for the operational environment OE.CGA\_SSCD\_Auth and OE.CGA\_TC\_SVD\_Imp from [PP-SSCD4]
- 5) The SFRs specified in this ST includes all security functional requirements (SFRs) specified in the core PPs [PP-SSCD2] and [PP-SSCD3]. Additional SFRs address :
  - a. trusted channel between the TOE and the SCA from [PP-SSCD5] and [PP-SSCD6]: FDP\_UIT.1/DTBS, FTP\_ITC.1/VAD and FTP\_ITC.1/DTBS.
  - b. Trusted communication with CGA from [PP-SSCD4] : FIA\_API.1 and FDP\_DAU.2/SVD, FTP\_ITC.1/SVD

	<b>Security Target Lite IDeal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>34/142</b>
---	--	--

- 6) This ST provides refinements for the SFR FIA\_UAU.1 according to [PP-SSCD4], [PP-SSCD5] and [PP-SSCD6].
- 7) The security assurance requirements (SARs) are originally taken from SARs of part 3 [CC3] according to the package conformance EAL 5 augmented with ALC\_DVS.2 and AVA\_VAN.5 (the Evaluation Assurance Level EAL5+ of the current ST exceeds the EAL4+ defined by [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6]).
- 8) The additional functionalities (PACE authentication, Chip Authentication Protocol Version 2 and Terminal Authentication Protocol Version 2) have been added to the TOE with: (i) additional security problem definition; (ii) additional security objectives; (iii) additional SFRs. All these additions are inspired from the [EAC2-PP]. Notice that the added security objectives for the operational environment don't mitigate any threats of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] and don't fulfil any OSPs meant to be addressed by security objectives for the TOE in PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6].

This security target is compliant with the SPD of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] as shown in the following table:

TOE SPDs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
<b>Assumptions</b>						
A.CGA	x		x	x		x
A.SCA	x		x	x		x
A.CSP		x			x	x
<b>Threats</b>						
T.SCD_Divulg	x	x	x	x	x	x
T.SCD_Derive	x	x	x	x	x	x
T.Hack_Phys	x	x	x	x	x	x
T.SVD_Forgery	x	x	x	x	x	x
T.SigF_Misuse	x	x	x	x	x	x
T.DTBS_Forgery	x	x	x	x	x	x
T.Sig_Forgery	x	x	x	x	x	x
<b>Organisational Security Policies</b>						
P.CSP_QCert	x	x	x	x	x	x
P.QSign	x	x	x	x	x	x
P.Sigy_SSCD	x	x	x	x	x	x
P.Sig_Non-Repud	x	x	x	x	x	x

**Table 1 PP SPDs vs. ST**

This security target is compliant with the security objectives of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] as shown in the following table:

TOE Objectives	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
<b>Objectives for the TOE</b>						
OT.Lifecycle_Security	x	x	x	x	x	x
OT.SCD/SVD_Auth_Gen	x		x	x		x
OT.SCD_Unique	x		x	x		x
OT.SCD_SVD_Corresp	x		x	x		x
OT.SCD_Secrecy	x	x	x	x	x	x
OT.Sig_Secure	x	x	x	x	x	x
OT.Sigy_SigF	x	x	x	x	x	x
OT.DTBS_Integrity_TOE	x	x	x	x	x	x
OT.EMSEC_Design	x	x	x	x	x	x
OT.Tamper_ID	x	x	x	x	x	x
OT.Tamper_Resistance	x	x	x	x	x	x
OT.TOE_TC_VAD_Imp				x	x	x
OT.TOE_TC_DTBS_Imp				x	x	x
OT.TOE_SSCD_Auth			x			x
OT.TOE_TC_SVD_Exp			x			x
OT.SCD_Auth_Imp		x			x	x
<b>Objectives for the Operational Environment</b>						

TOE Objectives	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
OE.SVD_Auth	x	x	x	x	x	x
OE.CGA_QCert	x	x	x	x	x	x
OE.SSCD_Prov_Service	x	x		x	x	
OE.SCD/SVD_Auth_Gen		x			x	x
OE.SCD_Unique		x			x	x
OE.SCD_SVD_Corresp		x			x	x
OE.SCD_Secrecy		x			x	x
OE.HID_VAD	x	x	x			
OE.DTBS_Intend	x	x	x	x	x	x
OE.DTBS_Protect	x	x	x			
OE.Signatory	x	x	x	x	x	x
OE.HID_TC_VAD_Exp				x	x	x
OE.SCA_TC_DTBS_Exp				x	x	x
OE.Dev_Prov_Service			x			x
OE.CGA_SSCD_Auth			x			x
OE.CGA_TC_SVD_Imp			x			x

**Table 2 PP Security Objectives vs. ST**

This security target is compliant with the security functional requirements of [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], [PP-SSCD6] as shown in the following table:

TOE SFRs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
FCS_CKM.1	x		x	x		x
FCS_CKM.4	x	x	x	x	x	x
FCS_COP.1	x	x	x	x	x	x
FDP_ACC.1/SCD/SVD_Generation	x		x	x		x
FDP_ACF.1/SCD/SVD_Generation	x		x	x		x
FDP_ACC.1/SVD_Transfer	x		x	x		x
FDP_ACF.1/SVD_Transfer	x		x	x		x
FDP_ACC.1/Signature_Creation	x	x	x	x	x	x
FDP_ACF.1/Signature_Creation	x	x	x	x	x	x
FDP_ACC.1/SCD_Import		x			x	x
FDP_ACF.1/SCD_Import		x			x	x
FDP_RIP.1	x	x	x	x	x	x
FDP_SDI.2/Persistent	x	x	x	x	x	x
FDP_SDI.2/DTBS	x	x	x	x	x	x
FIA_UID.1	x	x	x	x	x	x
FIA_UAU.1	x	x	x	x	x	x
FIA_AFL.1	x	x	x	x	x	x
FMT_SMR.1	x	x	x	x	x	x
FMT_SMF.1	x	x	x	x	x	x
FMT_MOF.1	x	x	x	x	x	x
FMT_MSA.1/Admin	x	x	x	x	x	x

TOE SFRs	PP SSCD2	PP SSCD3	PP SSCD4	PP SSCD5	PP SSCD6	Included
FMT_MSA.1/Signatory	x	x	x	x	x	x
FMT_MSA.2	x	x	x	x	x	x
FMT_MSA.3	x	x	x	x	x	x
FMT_MSA.4	x	x	x	x	x	x
FMT_MTD.1/Admin	x	x	x	x	x	x
FMT_MTD.1/Signatory	x	x	x	x	x	x
FPT_EMS.1	x	x	x	x	x	x
FPT_FLS.1	x	x	x	x	x	x
FPT_PHP.1	x	x	x	x	x	x
FPT_PHP.3	x	x	x	x	x	x
FPT_TST.1	x	x	x	x	x	x
FIA_API.1			x			x
FTP_ITC.1/SVD			x			x
FDP_DAU.2/SVD			x			x
FDP_UIT.1/DTBS				x	x	x
FTP_ITC.1/VAD				x	x	x
FTP_ITC.1/DTBS				x	x	x
FDP_ITC.1/SCD		x				x
FDP_UCT.1/SCD		x				x
FTP_ITC.1/SCD		x				x
FCS_RND.1						x

**Table 3 PP SFRs vs. ST**

## 6 Security Problem Definition

---

### 6.1 Assets

#### 6.1.1 Primary Assets

Following primary assets are protected by the TOE as listed below:

##### **D.SCD**

###### **Signature Creation Data**

Private key used to perform an electronic signature operation. The confidentiality, integrity and signatory's sole control over the use of the SCD must be maintained.

##### **D.SVD**

###### **Signature Verification Data**

Public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported must be maintained.

##### **D.DTBS/R**

###### **Data to be signed or its unique Representation**

Set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature must be maintained.

#### 6.1.2 Primary Assets related to EAC2

##### **Authenticity of the Electronic Documents Chip**

The authenticity of the electronic document's chip, personalized by the issuing state or organization for the electronic document holder, is used by the electronic document presenter to prove his possession of a genuine electronic document.

Generic Security Property: Authenticity

##### **Tracing Data**

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

Generic Security Property: Unavailability

##### **Sensitive User Data**

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

Generic Security Properties: Confidentiality, Integrity, Authenticity



	<b>Security Target Lite ID.eal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>41/142</b>
---	---	--

### **User Data stored on the TOE**

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

Generic Security Properties: Confidentiality, Integrity, Authenticity

### **User Data transferred between the TOE and the Terminal**

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

Generic Security Properties: Confidentiality, Integrity, Authenticity

### **6.1.3 Secondary Assets related to EAC2**

In order to achieve a sufficient protection of the primary assets, the following secondary assets also are protected by the TOE.

### **Accessibility of TOE Functions and Data only for Authorized Subjects**

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

Generic Security Property: Availability

### **Genuineness of the TOE**

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

Generic Security Property: Availability

### **Electronic Document Communication Establishment Authorization Data**

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

Restricted-revealable here refers to the fact that if necessary, the electronic document holder may reveal her verification values of CAN and MRZ to an authorized person, or to a device that acts according to respective regulations and is considered trustworthy.

Generic Security Properties: Confidentiality, Integrity

### **Secret Electronic Document Holder Authentication Data**

Secret authentication information for the electronic document holder being used for verification of the authentication attempts as authorized electronic document holder (sent PACE passwords, e.g. PIN or CAN).

Generic Security Properties: Confidentiality, Integrity

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

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

	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>42/142</b>
---	--	--

for such non-secret material is the document security object (SOD) that contains a digital signature.

Generic Security Properties: Integrity, Authenticity

## **TOE internal Secret Cryptographic Keys**

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

Generic Security Properties: Confidentiality, Integrity

*Application Note:*

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

## **6.2 Users / Subjects**

### **6.2.1 Users/Subjects related to EAC2**

#### **S.CSCA**

##### ***Country Signing Certification Authority***

An organization enforcing the policy of the electronic document issuer, i. e. confirming correctness of user and TSF data that are stored within the electronic document. The CSCA represents the country specific root of the public key infrastructure (PKI) for the electronic document, and creates Document Signer Certificates within this PKI. The CSCA also issues a self-signed CSCA certificate that has to be distributed to other countries by secure diplomatic means, see [ICAO9303].

#### **S.CVCA**

##### ***Country Verifying Certification Authority***

The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing state or organization, i. e. enforcing protection of sensitive user data that are stored in the electronic document. The CVCA represents the country specific root of the PKI of EAC2 terminals, and creates Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed as CVCA Link-Certificates, see [TR03110-3].

#### **S.DS**

##### ***Document Signer***

An organization enforcing the policy of the CSCA. A DS signs the Document Security Object (SOD) that is stored on the electronic document for Passive Authentication. A Document Signer is authorized by the national CSCA that issues Document Signer Certificates, see [ICAO9303]. Note that this role is usually delegated to a Personalization Agent.

 IDEMIA	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>43/142</b>
--	--	--

## **S.DV**

### ***Document Verifier***

An organization issuing terminal certificates. The DV is a Certificate Authority, authorized by the corresponding CVCA to issue certificates for EAC2 terminals, see [TR03110-3].

## **S.EDH**

### ***Electronic Document Holder***

A person who the electronic document issuer has personalized the electronic document for. Personalization here refers to associating a person uniquely with a specific electronic document. Note that an electronic document holder can also be an attacker.

## **S.EDP**

### ***Electronic Document Presenter***

A person presenting the electronic document to a terminal and claiming the identity of the electronic document holder. Note that an electronic document presenter can also be an attacker, cf. below.

## **S.Manufacturer**

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

## **S.PACE Terminal**

A PACE terminal implements the terminal part of the PACE protocol, and authenticates itself to the electronic document using a shared password (CAN, PIN, PUK or MRZ). A PACE terminal is not allowed to access sensitive user data.

## **S.Personalization Agent**

An organization acting on behalf of the electronic document issuer that personalizes the electronic document for the electronic document holder. Personalization includes some or all of the following activities: (i) establishing the identity of the electronic document holder for the biographic data in the electronic document, (ii) enrolling the biometric reference data of the electronic document holder, (iii) writing a subset of these data on the physical electronic document (optical personalization) and storing them within the electronic document's chip (electronic personalization), (iv) writing document meta data (i. e. document type, issuing country, expiry date, etc.) (v) writing the initial TSF data, and (vi) signing the Document Security Object, and the elementary files EF.CardSecurity and the EF.ChipSecurity (if applicable [ICAO9303], [TR03110-3]) in the role DS. Note that the role personalization agent may be distributed among several institutions according to the operational policy of the electronic document issuer.

## **S.EAC2 Terminal**

A terminal that has successfully passed Terminal Authentication 2 is an EAC2 terminal. It is authorized by the electronic document issuer through the Document Verifier of the receiving

	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>44/142</b>
---	--	--

branch (by issuing terminal certificates) to access a subset or all of the data stored on the electronic document.

## **S.Terminal**

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

### **6.2.2 Threat agents**

#### **S.Attacker**

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

### **6.2.3 Miscellaneous**

#### **S.User**

End user of the TOE who can be identified as administrator or signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.

#### **S.Admin**

User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.

#### **S.Signatory**

User who hold the TOE and use it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.

## **6.3 Threats**

### **6.3.1 Threats related to EAC2**

#### **T.Counterfeit/EAC2**

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

Threat agent:having high attack potential, being in possession of one or more legitimate ID-Cards

### **T.Sensitive\_Data**

An attacker tries to gain access to sensitive user data through the communication interface of the electronic document's chip. The attack T.Sensitive\_Data is similar to the threat T.Skimming from [PACEPP] w.r.t. the attack path (communication interface) and the motivation (to get data stored on the electronic document's chip) but differs from those in the asset under the attack (sensitive data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods.

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

### **T.Abuse-Func**

An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialisation and personalisation in the operational phase after delivery to the electronic document holder.

### **T.Eavesdropping**

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

### **T.Forgery**

An attacker fraudulently alters the User Data or/and TSF-data stored on the electronic document or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated BIS-PACE by means of changed electronic document holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.

### **T.Information\_Leakage**

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

### **T.Malfunction**

An attacker may cause a malfunction the electronic document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE's hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the electronic document outside the normal operating conditions, exploiting errors in the electronic document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>46/142</b>
---	--	--

## **T.Phys-Tamper**

An attacker may perform physical probing of the electronic document in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the electronic document in order to alter (I) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the electronic document.

## **T.Skimming**

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

## **T.Tracing**

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

### **6.3.2 Miscellaneous**

#### **T.SCD\_Divulg**

##### ***Storing, copying and releasing of the signature creation data***

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

#### **T.SCD\_Derive**

##### ***Derive the signature creation data***

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

#### **T.Hack\_Phys**

##### ***Physical attacks through the TOE interfaces***

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

#### **T.SVD\_Forgery**

##### ***Forgery of the signature verification data***

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

#### **T.SigF\_Misuse**

##### ***Misuse of the signature creation function of the TOE***

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

	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>47/142</b>
---	--	--

## **T.DTBS\_Forgery**

### ***Forgery of the DTBS/R***

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

## **T.Sig\_Forgery**

### ***Forgery of the electronic signature***

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

## **6.4 Organisational Security Policies**

### **6.4.1 OSP related to EAC2**

#### **P.EAC2\_Terminal**

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

#### **P.Terminal\_PKI**

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

#### **P.Card\_PKI**

PKI for Passive Authentication (issuing branch)

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

1.) The electronic document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the electronic document. For this aim, he runs a Country Signing Certification Authority (CSCA). The electronic document Issuer shall publish the CSCA Certificate (CCSCA).

2.) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (CCSCA) having to be made available to the electronic document Issuer by strictly secure means. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the electronic document Issuer.



	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>48/142</b>
---	--	--

3.) A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of electronic documents.

### **P.Manufact**

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

### **P.Pre-Operational**

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

### **P.Terminal**

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

- 1.) The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by electronic document holders.
- 2.) They shall implement the terminal parts of the PACE protocol, of the Passive Authentication and use them in this order. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
- 3.) The related terminals need not to use any own credentials.
- 4.) They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the electronic document).
- 5.) The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

### **P.Trustworthy\_PKI**

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



	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>49/142</b>
---	--	--

## 6.4.2 Miscellaneous

### P.CSP\_QCert

#### ***Qualified certificate***

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

### P.QSign

#### ***Qualified electronic signatures***

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

#### *Application Note:*

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

### P.Sigy\_SSCD

#### ***TOE as secure signature creation device***

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

### P.Sig\_Non-Repud

#### ***Non-repudiation of signatures***

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

## 6.5 Assumptions

### 6.5.1 All SSCD parts

#### A.CGA

##### *Trustworthy certificate generation application*

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

#### A.SCA

##### *Trustworthy signature creation application*

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

### 6.5.2 Parts 3 and 6 only

#### A.CSP

##### *Secure SCD/SVD management by CSP*

The CSP uses only a trustworthy SCD/SVD generation device and ensures that this device can be used by authorised user only. The CSP ensures that the SCD generated practically occurs only once, that generated SCD and SVD actually correspond to each other and that SCD cannot be derived from the SVD. The CSP ensures the confidentiality of the SCD during generation and export to the TOE, does not use the SCD for creation of any signature and irreversibly deletes the SCD in the operational environment after export to the TOE.

## 7 Security Objectives

---

### 7.1 Security Objectives for the TOE

#### 7.1.1 All SSCD parts

##### **OT.Tamper\_Resistance**

###### ***Tamper resistance***

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

##### **OT.Tamper\_ID**

###### ***Tamper detection***

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

##### **OT.EMSEC\_Design**

###### ***Provide physical emanations security***

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

##### **OT.DTBS\_Integrity\_TOE**

###### ***DTBS/R integrity inside the TOE***

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

##### **OT.Sigy\_SigF**

###### ***Signature creation function for the legitimate signatory only***

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

##### **OT.Sig\_Secure**

###### ***Cryptographic security of the electronic signature***

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

 IDEMIA	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>52/142</b>
--	--	--

## **OT.SCD\_Secrecy**

### ***Secrecy of the signature-creation data***

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

*Application Note:*

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

## **OT.Lifecycle\_Security**

### ***Lifecycle security***

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

*Application Note:*

The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD generation. The signatory shall be able to destroy the SCD stored in the SSCD e.g. after the (qualified) certificate for the corresponding SVD has been expired.

### **7.1.2 SSCD parts 2, 4 and 5 only**

## **OT.SCD\_SVD\_Corresp**

### ***Correspondence between SVD and SCD***

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

## **OT.SCD\_Unique**

### ***Uniqueness of the signature creation data***

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

## **OT.SCD/SVD\_Gen**

### ***Authorized SCD/SVD generation***

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

### **7.1.3 SSCD parts 3 and 6 only**

## **OT.SCD\_Auth\_Imp**

### ***Authorized SCD import***

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

*Application Note:*

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

	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>53/142</b>
---	--	--

#### 7.1.4 *SSCD part 4 only*

##### **OT.TOE\_SSCD\_Auth**

###### ***Authentication proof as SSCD***

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

##### **OT.TOE\_TC\_SVD\_Exp**

###### ***TOE trusted channel for SVD export***

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

#### 7.1.5 *SSCD parts 5 and 6 only*

##### **OT.TOE\_TC\_VAD\_Imp**

###### ***Trusted channel of TOE for VAD import***

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

###### *Application Note:*

This security objective for the TOE is partly covering OE.HID\_VAD from the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI). While OE.HID\_VAD in the core PP requires only the operational environment to protect VAD, this ST requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID\_TC\_VAD\_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE\_TC\_VAD\_Imp. Therefore this ST re-assigns partly the VAD protection from the operational environment as described by OE.HID\_VAD to the TOE as described by OT.TOE\_TC\_VAD\_Imp and leaves only the necessary functionality by the HID.

##### **OT.TOE\_TC\_DTBS\_Imp**

###### ***Trusted channel of TOE for DTBS import***

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

#### 7.1.6 *Security Objectives OT related to EAC2*

##### **OT.AC\_Pers\_EAC2**

###### ***Personalization of the Electronic Document***

The TOE must ensure that user data and TSF-Data that are permanently stored in the TOE can be written by authorized personalization agents only, with the following exception: An EAC2 terminal may also write or modify user data according to its effective access rights. The access rights are determined by the electronic document during Terminal Authentication 2. Justification: This security objective for the TOE modifies OT.AC\_Pers

	<b>Security Target Lite IDeal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>54/142</b>
---	--	--

from [PACEPP] as the additional features of EAC2 allow a strongly controlled, secure and fine-grained access to individual data groups of the electronic document.

## **OT.CA2**

### ***Proof of the Electronic Document's Chip Authenticity***

The TOE must allow EAC2 terminals to verify the identity and authenticity of the electronic document's chip as being issued by the identified issuing state or organization by Chip Authentication 2 [TR03110-2]. The authenticity of the chip and its proof mechanism provided by the electronic document's chip shall be protected against attacks with high attack potential.

## **OT.Sens\_Data\_EAC2**

### ***Confidentiality of sensitive User Data***

The TOE must ensure confidentiality of sensitive user data by granting access to sensitive data only to EAC2 terminals with corresponding access rights. The authorization of an EAC2 terminal is the minimum set of the access rights drawn from the terminal certificate used for successful authentication and the corresponding DV and CVCA certificates, and the access rights sent to the electronic document as part of PACE. The TOE must ensure confidentiality of all user data during transmission to an EAC2 terminal after Chip Authentication 2. Confidentiality of sensitive user data shall be protected against attacks with high attack potential.

## **OT.Data\_Authenticity**

### ***Authenticity of Data***

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

## **OT.Data\_Confidentiality**

### ***Confidentiality of Data***

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

## **OT.Data\_Integrity**

### ***Integrity of Data***

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

## OT.Identification

### *II*dentification of the TOE

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

## OT.Prot\_Abuse-Func

### *Protection against Abuse of Functionality*

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

## OT.Prot\_Inf\_Leak

### *Protection against Information Leakage*

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

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

#### *Application Note:*

This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

## OT.Prot\_Malfunction

### *Protection against Malfunctions*

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature. The following TOE security objectives address the aspects of identified threats to be countered involving TOE's environment.

## OT.Prot\_Phys-Tamper

### *Protection against Physical Tampering*

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

- o measuring through galvanic contacts representing a direct physical probing on the chip's surface except on pads being bonded (using standard tools for measuring voltage and current) or
- o measuring not using galvanic contacts, but other types of physical interaction between electrical charges (using tools used in solid-state physics research and IC failure analysis),

	<b>Security Target Lite ID.eal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>56/142</b>
---	---	--

- o manipulation of the hardware and its security functionality, as well as
- o controlled manipulation of memory contents (User Data, TSF-data) with a prior
- o reverse-engineering to understand the design and its properties and functionality.

## **OT.Tracing**

### ***Tracing electronic document***

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

#### *Application Note:*

Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the electronic document's chip (no Chip Authentication), a security objective like OT.Chip\_Auth\_Proof (proof of electronic document authenticity) cannot be achieved by the current TOE.

## **7.2 Security Objectives for the Operational Environment**

### **7.2.1 All SSCD parts**

#### **OE.Signatory**

##### ***Security obligation of the signatory***

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

#### **OE.DTBS\_Intend**

##### ***SCA sends data intended to be signed***

The signatory shall use a trustworthy SCA that

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

#### *Application Note:*

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



	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>57/142</b>
---	--	--

## OE.SVD\_Auth

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

## OE.CGA\_QCert

### **Generation of qualified certificates**

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

- o the name of the signatory controlling the TOE,
- o the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
- o the advanced signature of the CSP.

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

## 7.2.2 SSCD parts 3 and 6 only

## OE.SCD\_SVD\_Corresp

### **Correspondence between SVD and SCD**

The CSP shall ensure the correspondence between the SVD and the SCD generated by the CSP. This includes the correspondence between the SVD sent to the CGA and the SCD exported to the TOE of the signatory identified in the SVD certificate.

## OE.SCD\_Unique

### **Uniqueness of the signature creation data**

The CSP shall ensure the cryptographic quality of the SCD/SVD pair, which is generated in the environment, for the qualified or advanced electronic signature. The SCD used for signature creation shall practically occur only once, i.e. the probability of equal SCDs shall be negligible, and the SCD shall not be reconstructable from the SVD.

## OE.SCD\_Secrecy

### **SCD Secrecy**

The CSP shall protect the confidentiality of the SCD during generation and export to the TOE. The CSP shall not use the SCD for creation of any signature and shall irreversibly delete the SCD in the operational environment after export to the TOE.

## OE.SCD/SVD\_Auth\_Gen

### **Authorized SCD/SVD generation**

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

	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>58/142</b>
---	--	--

### 7.2.3 *SSCD part 4 only*

#### **OE.Dev\_Prov\_Service**

##### ***Authentic SSCD provided by SSCD Provisioning Service***

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

##### *Application Note:*

This objective replaces OE.SSCD\_Prov\_Service from the core PP, which is possible as it does not imply any additional requirements for the operational environment when compared to OE.SSCD\_Prov\_Service (OE.Dev\_Prov\_Service is a subset of OE.SSCD\_Prov\_Service).

#### **OE.CGA\_TC\_SVD\_Imp**

##### ***CGA trusted channel for SVD import***

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

#### **OE.CGA\_SSCD\_Auth**

##### ***Pre-initialisation of the TOE for SSCD authentication***

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

### 7.2.4 *SSCD parts 5 and 6 only*

#### **OE.HID\_TC\_VAD\_Exp**

##### ***Trusted channel of HID for VAD export***

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

##### *Application Note:*

This security objective for the TOE is partly covering OE.HID\_VAD from the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI). While OE.HID\_VAD in the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI) requires only the operational environment to protect VAD, this ST requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID\_TC\_VAD\_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE\_TC\_VAD\_Imp. Therefore this ST re-assigns partly the VAD protection from the operational environment as described by OE.HID\_VAD to the TOE as described by OT.TOE\_TC\_VAD\_Imp and leaves only the necessary functionality by the HID.

	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>59/142</b>
---	--	--

## **OE.SCA\_TC\_DTBS\_Exp**

### ***Trusted channel of SCA for DTBS export***

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

#### *Application Note:*

This security objective for the TOE is partly covering OE.DTBS\_Protect from the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI). While OE.DTBS\_Protect in the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI) requires only the operational environment to protect DTBS, this ST requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA\_TC\_DTBS\_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE\_TC\_DTBS\_Imp. Therefore this ST re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS\_Protect to the TOE as described by OT.TOE\_TC\_DTBS\_Imp and leaves only the necessary functionality by the SCA.

## **7.2.5 Security Objectives OE related to EAC2**

### **OE.Chip\_Auth\_Key**

#### ***Key Pairs needed for Chip Authentication***

The electronic document issuer has to ensure that the electronic document's chip authentication key pair is generated securely, that the private key of this key pair is stored correctly in the electronic document's chip, and that the corresponding public keys are distributed to the EAC2 terminals that are used according to [TR03110-2] to check the authenticity of the electronic document's chip. Justification: The TSF of [PACEPP] does not include any mechanism to verify the authenticity of an electronic document (i.e. protection against cloning). Therefore, this additional security objective for the operational environment does not mitigate any threat of, and does not fulfill any OSP of [PACEPP].

### **OE.Terminal\_Authentication**

#### ***Authentication Key pairs needed for Terminal Authentication***

The electronic document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the electronic document issuer shall run a Country Verifying Certification Authority. The instances of the PKI shall fulfill the requirements and rules of the corresponding certificate policy. The electronic document issuer shall make the CVCA certificate available to the personalization agent or the manufacturer. Justification: The TSF of [PACEPP] does not include any mechanism to verify the authenticity of the terminal that reads out the data stored on the electronic document (by successfully executing PACE, a terminal only proves knowledge of the PACE password). Therefore, this additional security objective for the operational environment does not mitigate any threat of, and does not fulfill any OSP of [PACEPP].

### **OE.Legislative\_Compliance**

#### ***Issuing of the electronic document***

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

## OE.Passive\_Auth\_Sign

### ***Authentication of electronic document by Signature***

The electronic document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the electronic document Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA Public Key (CCSCA). Hereby authenticity and integrity of these certificates are being maintained. A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine electronic documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on electronic document.

## OE.Personalisation

### ***Personalisation of electronic document***

The electronic document Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the electronic document holder and create the biographical data for the electronic document, (ii) enrol the biometric reference data of the electronic document holder, (iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the electronic document (electronic personalisation) for the electronic document holder, (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object (in the role of a DS).

## OE.Terminal

### ***Terminal operating***

The terminal operators must operate their terminals as follows:

- 1) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by electronic document holders.
- 2) The related terminals implement the terminal parts of the PACE protocol, of the Passive Authentication (by verification of the signature of the Document Security Object) and use them in this order. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
- 3) The related terminals need not to use any own credentials.
- 4) The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication of the electronic document (determination of the authenticity of data groups stored in the electronic document).
- 5) The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

## OE.Electronic\_Document\_Holder

### *Electronic document holder Obligations*

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

## 7.3 Security Objectives Rationale

### 7.3.1 Threats

#### 7.3.1.1 Threats related to EAC2

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

**T.Sensitive\_Data** The threat T.Sensitive\_Data is countered by the TOE-Objective OT.Sens\_Data\_EAC2, that requires that read access to sensitive user data is only granted to EAC2 terminals with corresponding access rights. Furthermore, it is required that the confidentiality of the data is ensured during transmission. The objective OE.Terminal\_Authentication requires the electronic document issuer to provide the public key infrastructure (PKI) to generate and distribute the card verifiable certificates needed by the electronic document to securely authenticate the EAC2 terminal.

**T.Abuse-Func** The threat T.Abuse-Func addresses attacks of misusing TOE's functionality to manipulate or to disclosure the stored User- or TSF-data as well as to disable or to bypass the soft-coded security functionality. The security objective OT.Prot\_Abuse-Func ensures that the usage of functions having not to be used in the operational phase is effectively prevented.

**T.Eavesdropping** The threat T.Eavesdropping addresses listening to the communication between the TOE and a PACE terminal or an EAC2 terminal in order to gain access to transferred user data. This threat is countered by the security objective OT.Data\_Confidentiality through a trusted channel based on PACE Authentication, and by OT.Sens\_Data\_EAC2 demanding a trusted channel that is based on Chip Authentication 2.

**T.Forgery** The threat T.Forgery addresses the fraudulent, complete or partial alteration of user data and/or TSF-Data stored on the TOE, and/or exchanged between the TOE and the terminal. The threat T.Forgery addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the terminal. The security objective OT.AC\_Pers requires the TOE to limit the write access for the electronic document to the trustworthy Personalisation Agent (cf. OE.Personalisation). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objectives OT.Data\_Integrity and OT.Data\_Authenticity, respectively. The objectives OT.Prot\_Phys-

Tamper and OT.Prot\_Abuse-Func contribute to protecting integrity of the User Data or/and TSF-data stored on the TOE. A terminal operator operating his terminals according to OE.Terminal and performing the Passive Authentication using the Document Security Object as aimed by OE.Passive\_Auth\_Sign will be able to effectively verify integrity and authenticity of the data received from the TOE. The threat is also addressed by the refinement of OT.AC\_Pers, here renamed OT.AC\_Pers\_EAC2.

**T.Information\_Leakage** The threats T.Information\_Leakage is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objectives OT.Prot\_Inf\_Leak.

**T.Malfunction** The threats T.Malfunction is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objectives OT.Prot\_Malfunction.

**T.Phys-Tamper** The threats T.Phys-Tamper is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objectives OT.Prot\_Phys-Tamper.

**T.Skimming** The threat T.Skimming addresses accessing the user data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless/contact-based interface. This threat is countered by the security objectives OT.Data\_Integrity, OT.Data\_Authenticity and OT.Data\_Confidentiality through the PACE authentication. The objective OE.Electronic\_Document\_Holder ensures that a PACE session can only be established either by the electronic document holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker. Additionally, the threat is also addressed by OT.Sens\_Data\_EAC2 that demands a trusted channel based on Chip Authentication 2, and requires that read access to sensitive user data is only granted to EAC2 terminals with corresponding access rights. Moreover, OE.Terminal\_Authentication requires the electronic document issuer to provide the corresponding PKI.

**T.Tracing** The threat T.Tracing addresses gathering TOE tracing data identifying it remotely by establishing or listening to a communication via the contactless/contact interface of the TOE, whereby the attacker does not a priori know the correct values of the PACE password. This threat is directly countered by security objectives OT.Tracing (no gathering TOE tracing data) and OE.Electronic\_Document\_Holder (the attacker does not a priori know the correct values of the shared passwords).

### 7.3.1.2 Miscellaneous

**T.SCD\_Divulg** addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the directive [DIR], recital (18). This threat is countered by

- o OE.SCD\_Secrecy, which assures the secrecy of the SCD in the CSP environment, and
- o OT.SCD\_Secrecy, which assures the secrecy of the SCD during use by the TOE for signature creation.



Furthermore, generation and/or import of SCD known by an attacker is countered by OE.SCD/SVD\_Auth\_Gen, which ensures that only authorized SCD generation in the environment is possible, and OT.SCD\_Auth\_Imp, which ensures that only authorised SCD import is possible.

**T.SCD\_Derive** deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD. OT.SCD/SVD\_Gen counters this threat by implementing cryptographically secure generation of the SCD/SVD pair. OT.Sig\_Secure ensures cryptographically secure electronic signatures. OE.SCD\_Unique counters this threat by implementing cryptographically secure generation of the SCD/SVD pair.

**T.Hack\_Phys** deals with physical attacks exploiting physical vulnerabilities of the TOE. OT.SCD\_Secrecy preserves the secrecy of the SCD. OT.EMSEC\_Design counters physical attacks through the TOE interfaces and observation of TOE emanations. OT.Tamper\_ID and OT.Tamper\_Resistance counter the threat T.Hack\_Phys by detecting and by resisting tampering attacks.

**T.SVD\_Forgery** deals with the forgery of the SVD exported by the TOE to the CGA for certificate generation. T.SVD\_Forgery is addressed by OT.SCD\_SVD\_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and OE.SVD\_Auth that ensures the integrity of the SVD exported by the TOE to the CGA.

OE.SCD\_SVD\_Corresp, which ensures correspondence between SVD and SCD.

Additionally T.SVD\_Forgery is addressed by OT.TOE\_TC\_SVD\_Exp, which ensures that the TOE sends the SVD in a verifiable form through a trusted channel to the CGA, as well as by OE.CGA\_TC\_SVD\_Imp, which provides verification of SVD authenticity by the CGA.

**T.SigF\_Misuse** addresses the threat of misuse of the TOE signature creation function to create SDO by others than the signatory to create an electronic signature on data for which the signatory has not expressed the intent to sign, as required by paragraph 1(c) of Annex III [DIR]. OT.Lifecycle\_Security (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by the signatory. OT.Sigy\_SigF (Signature creation function for the legitimate signatory only) ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS\_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign. OT.DTBS\_Integrity\_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. OE.Signatory ensures that the signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the signatory becomes control over the SSCD. OE.Signatory ensures also that the signatory keeps their VAD confidential.

The combination of OT.TOE\_TC\_DTBS\_Imp (Trusted channel of TOE for DTBS) and OE.SCA\_TC\_DTBS\_Exp (Trusted channel of SCA for DTBS) counters the undetected manipulation of the DTBS during the transmission from the SCA to the TOE.

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

	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>64/142</b>
---	--	--

OE.HID\_TC\_VAD\_Exp (Trusted channel of HID for VAD) and OT.TOE\_TC\_VAD\_Imp (Trusted channel of TOE for VAD).

**T.DTBS\_Forgery** addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function that does not represent the DTBS as presented to the signatory and for which the signature has expressed its intent to sign. The TOE IT environment addresses T.DTBS\_Forgery by the means of OE.DTBS\_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE. The TOE counters this threat by the means of OT.DTBS\_Integrity\_TOE by ensuring the integrity of the DTBS/R inside the TOE.

The threat T.DTBS\_Forgery is addressed by the security objectives OT.TOE\_TC\_DTBS\_Imp (Trusted channel of TOE for DTBS) and OE.SCA\_TC\_DTBS\_Exp (Trusted channel of SCA for DTBS), which ensure that the DTBS/R is sent through a trusted channel and cannot be altered undetected in transit between the SCA and the TOE.

**T.Sig\_Forgery** deals with non-detectable forgery of the electronic signature. OT.Sig\_Secure, OT.SCD\_Unique and OE.CGA\_QCert address this threat in general. OT.Sig\_Secure (Cryptographic security of the electronic signature) ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together. OT.SCD\_Unique ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. OE.CGA\_QCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

OE.SCD\_Unique ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance.

### 7.3.2 Organisational Security Policies

#### 7.3.2.1 OSP related to EAC2

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

**P.Terminal\_PKI** The OSP P.Terminal\_PKI is enforced by establishing the receiving PKI branch as aimed by the objective OE.Terminal\_Authentication.

**P.Card\_PKI** The OSP P.Card\_PKI is enforced by establishing the issuing PKI branch as aimed by the objectives OE.Passive\_Auth\_Sign (for the Document Security Object).

**P.Manufact** The OSP P.Manufact "Manufacturing of the electronic document's chip" requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalisation Data as being fulfilled by OT.Identification.

**P.Pre-Operational** The OSP P.Pre-Operational is enforced by the following security objectives:OT.Identification is affine to the OSP's property 'traceability before the



operational phase';OT.AC\_Pers and OE.Personalisation together enforce the OSP's properties 'correctness of the User- and the TSF-data stored' and 'authorisation of Personalisation Agents';OE.Legislative\_Compliance is affine to the OSP's property 'compliance with laws and regulations'. In addition, the threat is also addressed by the refinement of OT.AC\_Pers named OT.AC\_Pers\_EAC2.

**P.Terminal** The OSP P.Terminal is obviously enforced by the objective OE.Terminal, whereby the one-to-one mapping between the related properties is applicable.

**P.Trustworthy\_PKI** The OSP P.Trustworthy\_PKI is enforced by OE.Passive\_Auth\_Sign (for CSCA, issuing PKI branch).

### 7.3.2.2 Miscellaneous

**P.CSP\_QCert** establishes the CSP generating qualified certificate or non-qualified certificate linking the signatory and the SVD implemented in the SSCD under sole control of this signatory. P.CSP\_QCert is addressed by

- o OT.Lifecycle\_Security, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage,
- o OT.SCD\_SVD\_Corresp, which requires to ensure the correspondence between the SVD and the SCD during their generation,
- o OE.SCD/SVD\_Auth\_Gen, which ensures that the SCD/SVD generation can be invoked by authorized users only,
- o OT.SCD\_Auth\_Imp which ensures that authorised users only may invoke the import of the SCD,
- o OE.SCD\_SVD\_Corresp, which requires the CSP to ensure the correspondence between the SVD and the SCD during their generation, and
- o OE.CGA\_QCert for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the signatory.

According to OT.TOE\_SSCD\_Auth the copies of the TOE will hold unique identity and authentication data as SSCD and provide security mechanisms enabling the CGA to identify and to authenticate the TOE as SSCD to prove this identity as SSCD to the CGA. The OE.CGA\_SSCD\_Auth ensures that the SP checks the proof of the device presented of the applicant that it is a SSCD.

**P.QSign** provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy\_SigF ensures signatory's sole control of the SCD by requiring the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others. OT.Sig\_Secure ensures that the TOE creates electronic signatures, which cannot be forged without knowledge of the SCD through robust encryption techniques. OE.CGA\_QCert addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature. OE.DTBS\_Intend

ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

**P.Sigy\_SSCD** requires the TOE to meet Annex III [DIR]. This is ensured as follows:

- o OE.SCD\_Unique meets the paragraph 1(a) of the directive [DIR], Annex III, by the requirements that the SCD used for signature creation can practically occur only once;
- o OT.SCD\_Unique meets the paragraph 1(a) of Annex III [DIR], by the requirements that the SCD used for signature creation can practically occur only once;
- o OT.SCD\_Unique, OT.SCD\_Secrecy and OT.Sig\_Secure meet the requirement in paragraph 1(a) of Annex III [DIR] by the requirements to ensure secrecy of the SCD.
- o OT.EMSEC\_Design and OT.Tamper\_Resistance address specific objectives to ensure secrecy of the SCD against specific attacks;
- o OT.SCD\_Auth\_Imp, which limits SCD import to authorised users only;
- o OE.SCD\_Secrecy, which ensures the confidentiality of the SCD during generation and export to the TOE, and deletes the SCD after export to the TOE. The CSP does not use the SCD for signature creation;
- o OT.SCD\_Secrecy and OT.Sig\_Secure meet the requirement in paragraph 1(b) of Annex III [DIR] by the requirements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE;
- o OT.Sigy\_SigF meets the requirement in paragraph 1(c) of Annex III [DIR] by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others;
- o OT.DTBS\_Integrity\_TOE meets the requirements in paragraph 2 of Annex III [DIR] as the TOE must not alter the DTBS/R.

Paragraph 2 of Annex III [DIR], requires that an SSCD does not prevent the data to be signed from being presented to the signatory prior to the signature process is obviously fulfilled by the method of TOE usage: the SCA will present the DTBS to the signatory and send it to the SSCD for signing.

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

- o OT.Lifecycle\_Security requiring the TOE to detect flaws during the initialisation, personalisation and operational usage,
- o OE.SCD/SVD\_Auth\_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only,
- o OT.SCD/SVD\_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only, and
- o OT.Sigy\_SigF, which requires the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others.

OE.Dev\_Prov\_Service ensures that the legitimate user obtains a TOE sample as an authentic, initialised and personalised TOE from an SSCD Provisioning Service through the TOE delivery procedure. If the TOE implements SCD generated under control of the SSCD Provisioning Service the legitimate user receives the TOE as SSCD. If the TOE is delivered to the legitimate user without SCD In the operational phase he or she applies for the (qualified) certificate as the Device holder and legitimate user of the TOE. The CSP will use

the TOE security feature (addressed by the security objectives OT.TOE\_SSCD\_Auth and OT.TOE\_TC\_SVD\_Exp) to check whether the device presented is a SSCD linked to the applicant as required by OE.CGA\_SSCD\_Auth and the received SVD is sent by this SSCD as required by OE.CGA\_TC\_SVD\_Imp. Thus the obligation of the SSCD provision service for the first SCD/SVD pair is complemented in an appropriate way by the CSP for the SCD/SVD pair generated outside the secure preparation environment.

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

OE.SCD/SVD\_Auth\_Gen, OE.SCD\_Secrecy and OE.SCD\_Unique ensure the security of the SCD in the CSP environment. OE.SCD\_Secrecy ensures the confidentiality of the SCD during generation, during and after export to the TOE. The CSP does not use the SCD for creation of any signature and deletes the SCD irreversibly after export to the TOE. OE.SCD\_Unique provides that the signatory's SCD can practically occur just once. OE.SCD\_SVD\_Corresp ensures that the SVD in the certificate of the signatory corresponds to the SCD that is implemented in the copy of the TOE of the signatory. OE.CGA\_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. OE.SVD\_Auth and OE.CGA\_QCert require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory. OT.SCD\_SVD\_Corresp ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. OT.SCD\_Unique provides that the signatory's SCD can practically occur just once. OE.Signatory ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD). OT.Sigy\_SigF provides that only the signatory may use the TOE for signature creation. As prerequisite OE.Signatory ensures that the signatory keeps their VAD confidential. OE.DTBS\_Intend and OT.DTBS\_Integrity\_TOE ensure that the TOE creates electronic signatures only for those DTBS/R, which the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig\_Secure ensure that only this SCD may create a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle\_Security (Lifecycle security), OT.SCD\_Secrecy (Secrecy of the signature creation data), OT.EMSEC\_Design (Provide physical emanations security), OT.Tamper\_ID (Tamper detection) and OT.Tamper\_Resistance (Tamper resistance) protect the SCD against any compromise.

The TOE security feature addressed by the security objectives OT.TOE\_SSCD\_Auth and OT.TOE\_TC\_SVD\_Exp supported by OE.Dev\_Prov\_Service enables the verification whether the device presented by the applicant is a SSCD as required by OE.CGA\_SSCD\_Auth and the received SVD is sent by the device holding the corresponding SCD as required by OE.CGA\_TC\_SVD\_Imp.

The confidentiality of VAD is protected during the transmission between the HI device and TOE according to OE.HID\_TC\_VAD\_Exp (Trusted channel of HID for VAD) and OT.TOE\_TC\_VAD\_Imp (Trusted channel of TOE for VAD). OE.DTBS\_Intend (SCA sends data intended to be signed), OT.DTBS\_Integrity\_TOE (DTBS/R integrity inside the TOE), OE.SCA\_TC\_DTBS\_Exp (Trusted channel of SCA for DTBS) and OT.TOE\_TC\_DTBS\_Imp (Trusted channel of TOE for DTBS) ensure that the TOE generates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS.

### 7.3.3 Assumptions

#### 7.3.3.1 All SSCD parts

**A.CGA** establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA\_QCert (Generation of qualified certificates), which ensures the generation of qualified certificates, and by OE.SVD\_Auth (Authenticity of the SVD), which ensures the protection of the integrity of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

**A.SCA** establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by OE.DTBS\_Intend (Data intended to be signed) which ensures that the SCA generates the DTBS/R of the data that have been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE.

#### 7.3.3.2 Parts 3 and 6 only

**A.CSP** establishes several security aspects concerning handling of SCD and SVD by the CSP. That the SCD/SVD generation device can only be used by authorized users is addressed by OE.SCD/SVD\_Auth\_Gen (Authorized SCD/SVD Generation), that the generated SCD is unique and cannot be derived by the SVD is addressed by OE.SCD\_Unique (Uniqueness of the signature creation data), that SCD and SVD correspond to each other is addressed by OE.SCD\_SVD\_Corresp (Correspondence between SVD and SCD), and that the SCD are kept confidential, are not used for signature generation in the environment and are deleted in the environment once exported to the TOE is addressed by OE.SCD\_Secrecy (SCD Secrecy).

### 7.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
<a href="#">T.Counterfeit/EAC2</a>	<a href="#">OT.CA2</a> , <a href="#">OE.Chip Auth Key</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Sensitive Data</a>	<a href="#">OT.Sens Data EAC2</a> , <a href="#">OE.Terminal Authentication</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Abuse-Func</a>	<a href="#">OT.Prot Abuse-Func</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Eavesdropping</a>	<a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Sens Data EAC2</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Forgery</a>	<a href="#">OT.AC Pers EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Prot Abuse-Func</a> , <a href="#">OT.Prot Phys-Tamper</a> , <a href="#">OE.Personalisation</a> , <a href="#">OE.Passive Auth Sign</a> , <a href="#">OE.Terminal</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Information Leakage</a>	<a href="#">OT.Prot Inf Leak</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Malfunction</a>	<a href="#">OT.Prot Malfunction</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Phys-Tamper</a>	<a href="#">OT.Prot Phys-Tamper</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Skimming</a>	<a href="#">OT.Data Integrity</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Sens Data EAC2</a> , <a href="#">OE.Terminal Authentication</a> , <a href="#">OE.Electronic Document Holder</a>	<a href="#">Section 7.3.1</a>

<a href="#">T.Tracing</a>	<a href="#">OT.Tracing</a> , <a href="#">OE.Electronic Document Holder</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.SCD Divulg</a>	<a href="#">OT.SCD Secrecy</a> , <a href="#">OT.SCD Auth Imp</a> , <a href="#">OE.SCD/SVD Auth Gen</a> , <a href="#">OE.SCD Secrecy</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.SCD Derive</a>	<a href="#">OT.SCD/SVD Gen</a> , <a href="#">OT.Sig Secure</a> , <a href="#">OE.SCD Unique</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Hack Phys</a>	<a href="#">OT.SCD Secrecy</a> , <a href="#">OT.EMSEC Design</a> , <a href="#">OT.Tamper ID</a> , <a href="#">OT.Tamper Resistance</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.SVD Forgery</a>	<a href="#">OT.SCD SVD Corresp</a> , <a href="#">OE.SVD Auth</a> , <a href="#">OE.SCD SVD Corresp</a> , <a href="#">OT.TOE TC SVD Exp</a> , <a href="#">OE.CGA TC SVD Imp</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.SigF Misuse</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.DTBS Integrity TOE</a> , <a href="#">OE.Signatory</a> , <a href="#">OE.DTBS Intend</a> , <a href="#">OT.TOE TC VAD Imp</a> , <a href="#">OT.TOE TC DTBS Imp</a> , <a href="#">OE.HID TC VAD Exp</a> , <a href="#">OE.SCA TC DTBS Exp</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.DTBS Forgery</a>	<a href="#">OT.DTBS Integrity TOE</a> , <a href="#">OE.DTBS Intend</a> , <a href="#">OT.TOE TC DTBS Imp</a> , <a href="#">OE.SCA TC DTBS Exp</a>	<a href="#">Section 7.3.1</a>
<a href="#">T.Sig Forgery</a>	<a href="#">OT.SCD Unique</a> , <a href="#">OT.Sig Secure</a> , <a href="#">OE.CGA QCert</a> , <a href="#">OE.SCD Unique</a>	<a href="#">Section 7.3.1</a>

**Table 4 Threats and Security Objectives - Coverage**

Security Objectives	Threats	Rationale
<a href="#">OT.Tamper Resistance</a>	<a href="#">T.Hack Phys</a>	
<a href="#">OT.Tamper ID</a>	<a href="#">T.Hack Phys</a>	
<a href="#">OT.EMSEC Design</a>	<a href="#">T.Hack Phys</a>	
<a href="#">OT.DTBS Integrity TOE</a>	<a href="#">T.SigF Misuse</a> , <a href="#">T.DTBS Forgery</a>	
<a href="#">OT.Sigy SigF</a>	<a href="#">T.SigF Misuse</a>	
<a href="#">OT.Sig Secure</a>	<a href="#">T.SCD Derive</a> , <a href="#">T.Sig Forgery</a>	
<a href="#">OT.SCD Secrecy</a>	<a href="#">T.SCD Divulg</a> , <a href="#">T.Hack Phys</a>	
<a href="#">OT.Lifecycle Security</a>	<a href="#">T.SigF Misuse</a>	
<a href="#">OT.SCD SVD Corresp</a>	<a href="#">T.SVD Forgery</a>	
<a href="#">OT.SCD Unique</a>	<a href="#">T.Sig Forgery</a>	
<a href="#">OT.SCD/SVD Gen</a>	<a href="#">T.SCD Derive</a>	
<a href="#">OT.SCD Auth Imp</a>	<a href="#">T.SCD Divulg</a>	
<a href="#">OT.TOE SSCD Auth</a>		
<a href="#">OT.TOE TC SVD Exp</a>	<a href="#">T.SVD Forgery</a>	
<a href="#">OT.TOE TC VAD Imp</a>	<a href="#">T.SigF Misuse</a>	
<a href="#">OT.TOE TC DTBS Imp</a>	<a href="#">T.SigF Misuse</a> , <a href="#">T.DTBS Forgery</a>	

<a href="#">OT.AC Pers EAC2</a>	<a href="#">T.Forgery</a>	
<a href="#">OT.CA2</a>	<a href="#">T.Counterfeit/EAC2</a>	
<a href="#">OT.Sens Data EAC2</a>	<a href="#">T.Sensitive Data</a> , <a href="#">T.Eavesdropping</a> , <a href="#">T.Skimming</a>	
<a href="#">OT.Data Authenticity</a>	<a href="#">T.Forgery</a> , <a href="#">T.Skimming</a>	
<a href="#">OT.Data Confidentiality</a>	<a href="#">T.Eavesdropping</a> , <a href="#">T.Skimming</a>	
<a href="#">OT.Data Integrity</a>	<a href="#">T.Forgery</a> , <a href="#">T.Skimming</a>	
<a href="#">OT.Identification</a>		
<a href="#">OT.Prot Abuse-Func</a>	<a href="#">T.Abuse-Func</a> , <a href="#">T.Forgery</a>	
<a href="#">OT.Prot Inf Leak</a>	<a href="#">T.Information Leakage</a>	
<a href="#">OT.Prot Malfunction</a>	<a href="#">T.Malfunction</a>	
<a href="#">OT.Prot Phys-Tamper</a>	<a href="#">T.Forgery</a> , <a href="#">T.Phys-Tamper</a>	
<a href="#">OT.Tracing</a>	<a href="#">T.Tracing</a>	
<a href="#">OE.Signatory</a>	<a href="#">T.SigF Misuse</a>	
<a href="#">OE.DTBS Intend</a>	<a href="#">T.SigF Misuse</a> , <a href="#">T.DTBS Forgery</a>	
<a href="#">OE.SVD Auth</a>	<a href="#">T.SVD Forgery</a>	
<a href="#">OE.CGA QCert</a>	<a href="#">T.Sig Forgery</a>	
<a href="#">OE.SCD SVD Corresp</a>	<a href="#">T.SVD Forgery</a>	
<a href="#">OE.SCD Unique</a>	<a href="#">T.SCD Derive</a> , <a href="#">T.Sig Forgery</a>	
<a href="#">OE.SCD Secrecy</a>	<a href="#">T.SCD Divulg</a>	
<a href="#">OE.SCD/SVD Auth Gen</a>	<a href="#">T.SCD Divulg</a>	
<a href="#">OE.Dev Prov Service</a>		
<a href="#">OE.CGA TC SVD Imp</a>	<a href="#">T.SVD Forgery</a>	
<a href="#">OE.CGA SSCD Auth</a>		
<a href="#">OE.HID TC VAD Exp</a>	<a href="#">T.SigF Misuse</a>	
<a href="#">OE.SCA TC DTBS Exp</a>	<a href="#">T.SigF Misuse</a> , <a href="#">T.DTBS Forgery</a>	
<a href="#">OE.Chip Auth Key</a>	<a href="#">T.Counterfeit/EAC2</a>	
<a href="#">OE.Terminal Authentication</a>	<a href="#">T.Sensitive Data</a> , <a href="#">T.Skimming</a>	
<a href="#">OE.Legislative Compliance</a>		
<a href="#">OE.Passive Auth Sign</a>	<a href="#">T.Forgery</a>	
<a href="#">OE.Personalisation</a>	<a href="#">T.Forgery</a>	
<a href="#">OE.Terminal</a>	<a href="#">T.Forgery</a>	
<a href="#">OE.Electronic Document Holder</a>	<a href="#">T.Skimming</a> , <a href="#">T.Tracing</a>	

**Table 5 Security Objectives and Threats - Coverage**

Organisational Security Policies	Security Objectives	Rationale
<a href="#">P.EAC2 Terminal</a>	<a href="#">OE.Terminal</a> , <a href="#">OE.Chip Auth Key</a> , <a href="#">OE.Terminal Authentication</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Terminal PKI</a>	<a href="#">OE.Terminal Authentication</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Card PKI</a>	<a href="#">OE.Passive Auth Sign</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Manufact</a>	<a href="#">OT.Identification</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Pre-Operational</a>	<a href="#">OT.Identification</a> , <a href="#">OT.AC Pers EAC2</a> , <a href="#">OE.Personalisation</a> , <a href="#">OE.Legislative Compliance</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Terminal</a>	<a href="#">OE.Terminal</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Trustworthy PKI</a>	<a href="#">OE.Passive Auth Sign</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.CSP QCert</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD SVD Corresp</a> , <a href="#">OE.CGA QCert</a> , <a href="#">OT.SCD Auth Imp</a> , <a href="#">OE.SCD/SVD Auth Gen</a> , <a href="#">OE.SCD SVD Corresp</a> , <a href="#">OT.TOE SSCD Auth</a> , <a href="#">OE.CGA SSCD Auth</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.QSign</a>	<a href="#">OT.Sig Secure</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OE.CGA QCert</a> , <a href="#">OE.DTBS Intend</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Sigy SSCD</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD/SVD Gen</a> , <a href="#">OT.SCD Unique</a> , <a href="#">OT.SCD Secrecy</a> , <a href="#">OT.Sig Secure</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.DTBS Integrity TOE</a> , <a href="#">OT.EMSEC Design</a> , <a href="#">OT.Tamper Resistance</a> , <a href="#">OT.SCD Auth Imp</a> , <a href="#">OE.SCD/SVD Auth Gen</a> , <a href="#">OE.SCD Secrecy</a> , <a href="#">OE.SCD Unique</a> , <a href="#">OT.TOE SSCD Auth</a> , <a href="#">OT.TOE TC SVD Exp</a> , <a href="#">OE.Dev Prov Service</a> , <a href="#">OE.CGA TC SVD Imp</a> , <a href="#">OE.CGA SSCD Auth</a>	<a href="#">Section 7.3.2</a>
<a href="#">P.Sig Non-Repud</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.SCD Unique</a> , <a href="#">OT.SCD SVD Corresp</a> , <a href="#">OT.SCD Secrecy</a> , <a href="#">OT.Sig Secure</a> , <a href="#">OT.Sigy SigF</a> , <a href="#">OT.DTBS Integrity TOE</a> , <a href="#">OT.EMSEC Design</a> , <a href="#">OT.Tamper ID</a> , <a href="#">OT.Tamper Resistance</a> , <a href="#">OE.CGA QCert</a> , <a href="#">OE.SVD Auth</a> , <a href="#">OE.DTBS Intend</a> , <a href="#">OE.Signatory</a> , <a href="#">OE.SCD/SVD Auth Gen</a> , <a href="#">OE.SCD Secrecy</a> , <a href="#">OE.SCD Unique</a> , <a href="#">OE.SCD SVD Corresp</a> , <a href="#">OT.TOE SSCD Auth</a> , <a href="#">OT.TOE TC SVD Exp</a> , <a href="#">OE.Dev Prov Service</a> , <a href="#">OE.CGA TC SVD Imp</a> , <a href="#">OE.CGA SSCD Auth</a> , <a href="#">OT.TOE TC VAD Imp</a> , <a href="#">OT.TOE TC DTBS Imp</a> , <a href="#">OE.HID TC VAD Exp</a> , <a href="#">OE.SCA TC DTBS Exp</a>	<a href="#">Section 7.3.2</a>

**Table 6 OSPs and Security Objectives - Coverage**



Security Objectives	Organisational Security Policies	Rationale
<a href="#">OT.Tamper Resistance</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OT.Tamper ID</a>	<a href="#">P.Sig_Non-Repud</a>	
<a href="#">OT.EMSEC Design</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OT.DTBS Integrity TOE</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OT.Sigy_SigF</a>	<a href="#">P.QSign</a> , <a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OT.Sig Secure</a>	<a href="#">P.QSign</a> , <a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OT.SCD Secrecy</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OT.Lifecycle Security</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OT.SCD_SVD Corresp</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OT.SCD Unique</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OT.SCD/SVD Gen</a>	<a href="#">P.Sigy_SSCD</a>	
<a href="#">OT.SCD Auth Imp</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.Sigy_SSCD</a>	
<a href="#">OT.TOE SSCD Auth</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OT.TOE TC SVD Exp</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OT.TOE TC VAD Imp</a>	<a href="#">P.Sig_Non-Repud</a>	
<a href="#">OT.TOE TC DTBS Imp</a>	<a href="#">P.Sig_Non-Repud</a>	
<a href="#">OT.AC Pers EAC2</a>	<a href="#">P.Pre-Operational</a>	
<a href="#">OT.CA2</a>		
<a href="#">OT.Sens Data EAC2</a>		
<a href="#">OT.Data Authenticity</a>		
<a href="#">OT.Data Confidentiality</a>		
<a href="#">OT.Data Integrity</a>		
<a href="#">OT.Identification</a>	<a href="#">P.Manufact</a> , <a href="#">P.Pre-Operational</a>	
<a href="#">OT.Prot Abuse-Func</a>		
<a href="#">OT.Prot Inf Leak</a>		
<a href="#">OT.Prot Malfunction</a>		
<a href="#">OT.Prot Phys-Tamper</a>		
<a href="#">OT.Tracing</a>		
<a href="#">OE.Signatory</a>	<a href="#">P.Sig_Non-Repud</a>	
<a href="#">OE.DTBS Intend</a>	<a href="#">P.QSign</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OE.SVD Auth</a>	<a href="#">P.Sig_Non-Repud</a>	
<a href="#">OE.CGA_QCert</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.QSign</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OE.SCD_SVD Corresp</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.Sig_Non-Repud</a>	



<a href="#">OE.SCD Unique</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OE.SCD Secrecy</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OE.SCD/SVD Auth Gen</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OE.Dev Prov Service</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OE.CGA TC SVD Imp</a>	<a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OE.CGA SSCD Auth</a>	<a href="#">P.CSP_QCert</a> , <a href="#">P.Sigy_SSCD</a> , <a href="#">P.Sig_Non-Repud</a>	
<a href="#">OE.HID TC VAD Exp</a>	<a href="#">P.Sig_Non-Repud</a>	
<a href="#">OE.SCA TC DTBS Exp</a>	<a href="#">P.Sig_Non-Repud</a>	
<a href="#">OE.Chip Auth Key</a>	<a href="#">P.EAC2_Terminal</a>	
<a href="#">OE.Terminal Authentication</a>	<a href="#">P.EAC2_Terminal</a> , <a href="#">P.Terminal_PKI</a>	
<a href="#">OE.Legislative Compliance</a>	<a href="#">P.Pre-Operational</a>	
<a href="#">OE.Passive Auth Sign</a>	<a href="#">P.Card_PKI</a> , <a href="#">P.Trustworthy_PKI</a>	
<a href="#">OE.Personalisation</a>	<a href="#">P.Pre-Operational</a>	
<a href="#">OE.Terminal</a>	<a href="#">P.EAC2_Terminal</a> , <a href="#">P.Terminal</a>	
<a href="#">OE.Electronic Document Holder</a>		

**Table 7 Security Objectives and OSPs - Coverage**

Assumptions	Security Objectives for the Operational Environment	Rationale
<a href="#">A.CGA</a>	<a href="#">OE.CGA_QCert</a> , <a href="#">OE.SVD Auth</a>	<a href="#">Section 7.3.3</a>
<a href="#">A.SCA</a>	<a href="#">OE.DTBS Intend</a>	<a href="#">Section 7.3.3</a>
<a href="#">A.CSP</a>	<a href="#">OE.SCD/SVD Auth Gen</a> , <a href="#">OE.SCD Secrecy</a> , <a href="#">OE.SCD Unique</a> , <a href="#">OE.SCD_SVD Corresp</a>	<a href="#">Section 7.3.3</a>

**Table 8 Assumptions and Security Objectives for the Operational Environment - Coverage**

Security Objectives for the Operational Environment	Assumptions	Rationale
<a href="#">OE.Signatory</a>		
<a href="#">OE.DTBS Intend</a>	<a href="#">A.SCA</a>	
<a href="#">OE.SVD Auth</a>	<a href="#">A.CGA</a>	
<a href="#">OE.CGA_QCert</a>	<a href="#">A.CGA</a>	
<a href="#">OE.SCD_SVD Corresp</a>	<a href="#">A.CSP</a>	
<a href="#">OE.SCD Unique</a>	<a href="#">A.CSP</a>	
<a href="#">OE.SCD Secrecy</a>	<a href="#">A.CSP</a>	
<a href="#">OE.SCD/SVD Auth Gen</a>	<a href="#">A.CSP</a>	
<a href="#">OE.Dev Prov Service</a>		

<a href="#">OE.CGA TC SVD Imp</a>		
<a href="#">OE.CGA SSCD Auth</a>		
<a href="#">OE.HID TC VAD Exp</a>		
<a href="#">OE.SCA TC DTBS Exp</a>		
<a href="#">OE.Chip Auth Key</a>		
<a href="#">OE.Terminal Authentication</a>		
<a href="#">OE.Legislative Compliance</a>		
<a href="#">OE.Passive Auth Sign</a>		
<a href="#">OE.Personalisation</a>		
<a href="#">OE.Terminal</a>		
<a href="#">OE.Electronic Document Holder</a>		

**Table 9 Security Objectives for the Operational Environment and Assumptions - Coverage**

## 8 Extended Requirements

---

### 8.1 Extended Family FPT\_EMS - TOE Emanation

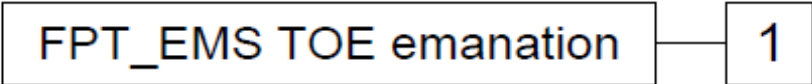
The additional family FPT\_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE’s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT\_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation.

The family “TOE Emanation (FPT\_EMS)” is specified as follows:

Family behavior:

This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT\_EMS.1 TOE emanation has two constituents:

FPT\_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT\_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT\_EMS.1  
There are no management activities foreseen.

Audit: FPT\_EMS.1  
There are no actions defined to be auditable if FAU\_GEN (Security audit data generation) is included in a PP or ST using FPT\_EMS.1.

<b>FPT_EMS.1 TOE Emanation</b>
--------------------------------

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

**8.2 Extended Family FIA\_API - Authentication Proof of Identity**

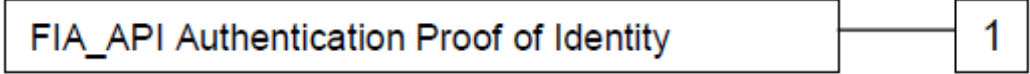
To describe the IT security functional requirements of the TOE a sensitive family (FIA\_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external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

The family "Authentication Proof of Identity (FIA\_API)" is specified as follows:

Family behavior:

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

Component levelling:



FIA\_API.1                      Authentication Proof of Identity.

Management:              FIA\_API.1

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

Audit:                              There are no actions defined to be auditable.

<b>FIA_API.1 Authentication Proof of Identity</b>
---

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA\_API.1.1** The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or role].

**8.3 Extended Family FCS\_RND - Generation of random numbers**

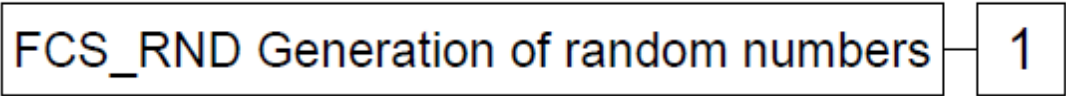
To describe the IT security functional requirements of the TOE, the family FCS\_RND of the class FCS (Cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS\_RND.1 is not limited to generation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

The family "Generation of random numbers (FCS\_RND)" is specified as follows:

Family behavior:

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component leveling:



FCS\_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS\_RND.1  
There are no management activities foreseen.

Audit: FCS\_RND.1  
There are no actions defined to be auditable.

<b>FCS_RND.1 Quality Metric for Random Numbers</b>
--

Hierarchical to: No other components.

Dependencies: No dependencies.

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

**8.4 Extended Family FMT\_LIM - Limited capabilities**

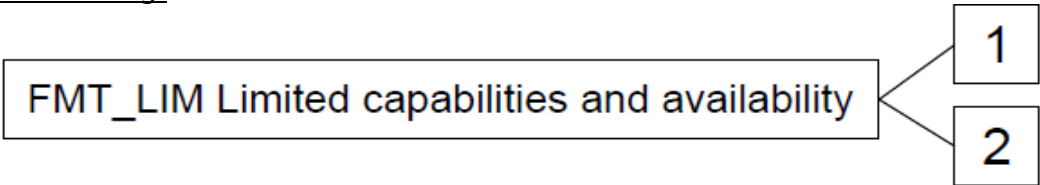
The family FMT\_LIM describes the functional requirements for the test features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class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

The family "Limited capabilities and availability (FMT\_LIM)" is specified as follows:

Family behavior:

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP\_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component leveling:



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

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

Management: FMT\_LIM.1, FMT\_LIM.2  
There are no management activities foreseen.

Audit: FMT\_LIM.1, FMT\_LIM.2  
There are no actions defined to be auditable.

### **FMT\_LIM.1 Limited Capabilities**

Hierarchical to: No other components.

Dependencies: FMT\_LIM.2 Limited availability.

**FMT\_LIM.1.1** The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT\_LIM.2)" the following policy is enforced [assignment: Limited capability and availability policy].

### **FMT\_LIM.2 Limited Availability**

Hierarchical to: No other components.

Dependencies: FMT\_LIM.1 Limited capabilities.

**FMT\_LIM.2.1** The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT\_LIM.1)" the following policy is enforced [assignment: Limited capability and availability policy].

## 9 Security Requirements

---

### 9.1 Security Functional Requirements

This section describes the requirements imposed on the TOE in order to achieve the security objectives laid down in the previous chapter.

#### 9.1.1 All SSCD parts

##### 9.1.1.1 Protection of the TSF (FPT)

#### FPT\_EMS.1 TOE Emanation

**FPT\_EMS.1.1** The TOE shall not emit **side channel** in excess of **state of the art** enabling access to

- o **RAD,**
- o **the PIN, PUK,**
- o **the session keys (PACE-KMAC, PACE-KEnc), (CA-KMAC, CA-KEnc),**
- o **the ephemeral private key ephem - SKPICC- PACE,**
- o **the Chip Authentication private keys (SKPICC)**

and

- o **SCD.**

**FPT\_EMS.1.2** The TSF shall ensure **that unauthorized users** are unable to use the following interface **external circuit contacts** to gain access to

- o **RAD,**
- o **the PIN, PUK,**
- o **the session keys (PACE-KMAC, PACE-KEnc), (CA-KMAC, CA-KEnc),**
- o **the ephemeral private key ephem - SKPICC- PACE,**
- o **the Chip Authentication private keys (SKPICC)**

and

- o **SCD.**

#### *Application Note:*

This SFR covers the definition in SSCD PPs and extends them by session keys, keys and PIN/PUK as part of the EAC V2 protocol aspects. This extension does not conflict with the strict conformance to SSCD PPs.

The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing



of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.

Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

#### **FPT\_FLS.1 Failure with preservation of secure state**

**FPT\_FLS.1.1** The TSF shall preserve a secure state when the following types of failures occur:

- o **(1) self-test according to FPT\_TST fails**
- o **(2) power shortage**
- o **(3) over and under voltage**
- o **(4) over and under clock frequency**
- o **(5) over and under temperature**
- o **(6) integrity problems**
- o **(7) unexpected abortion of the execution of the TSF due to external events**
- o **No other failure.**

#### **FPT\_PHP.1 Passive detection of physical attack**

**FPT\_PHP.1.1** The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

**FPT\_PHP.1.2** The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

#### **FPT\_PHP.3 Resistance to physical attack**

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

### FPT\_TST.1 TSF testing

**FPT\_TST.1.1** The TSF shall run a suite of self tests **during initial start-up and periodically during normal operation** to demonstrate the correct operation of **the TSF**.

**FPT\_TST.1.2** The TSF shall provide authorised users with the capability to verify the integrity of **TSF data**.

**FPT\_TST.1.3** The TSF shall provide authorised users with the capability to verify the integrity of **TSF**.

#### 9.1.1.2 Security management (FMT)

### FMT\_SMR.1 Security roles

**FMT\_SMR.1.1** The TSF shall maintain the roles **R.Admin and R.Sigy**.

**FMT\_SMR.1.2** The TSF shall be able to associate users with roles.

### FMT\_SMF.1 Specification of Management Functions

**FMT\_SMF.1.1** The TSF shall be capable of performing the following management functions:

- o **Creation and modification of RAD,**
- o **Enabling the signature creation function,**
- o **Modification of the security attribute SCD/SVD management, SCD operational,**
- o **Change the default value of the security attribute SCD Identifier,**
- o **Initialization,**
- o **Pre-Personalization,**
- o **Personalization,**
- o **Configuration,**
- o **Resume and unblock the PIN and PUK (if any).**

*Application Note:*

This SFR covers the definition in SSCD PPs and extends them by EAC V2 protocol aspects. This extension does not conflict with the strict conformance to SSCD PPs.

**FMT\_MOF.1 Management of security functions behaviour**

**FMT\_MOF.1.1** The TSF shall restrict the ability to **enable** the functions **signature creation function** to **R.Sigy**.

**FMT\_MSA.1/Admin Management of security attributes**

**FMT\_MSA.1.1/Admin** The TSF shall enforce the **SCD/SVD Generation SFP and SCD Import SFP** to restrict the ability to **modify** the security attributes **SCD/SVD management** to **R.Admin**.

**FMT\_MSA.1/Signatory Management of security attributes**

**FMT\_MSA.1.1/Signatory** The TSF shall enforce the **Signature Creation SFP** to restrict the ability to **modify** the security attributes **SCD operational** to **R.Sigy**.

**FMT\_MSA.2 Secure security attributes**

**FMT\_MSA.2.1** The TSF shall ensure that only secure values are accepted for **SCD/SVD Management and SCD operational**.

**FMT\_MSA.3 Static attribute initialisation**

**FMT\_MSA.3.1** The TSF shall enforce the **SCD/SVD Generation SFP, SVD Transfer SFP, SCD Import SFP and Signature Creation SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

**FMT\_MSA.3.2** The TSF shall allow the **R.Admin** to specify alternative initial values to override the default values when an object or information is created.

**FMT\_MSA.4 Security attribute value inheritance**

**FMT\_MSA.4.1** The TSF shall use the following rules to set the value of security attributes:

- o (1) If **S.Admin** successfully generates an **SCD/SVD** pair without **S.Sigy** being authenticated the security attribute "**SCD operational of the SCD**" shall be set to "**no**" as a single operation
- o (2) If **S.Sigy** successfully generates an **SCD/SVD** pair the security attribute "**SCD operational of the SCD**" shall be set to "**yes**" as a single operation

- (3) If S.Admin imports SCD while S.Sigy is not currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "no" after import of the SCD as a single operation.
- (4) If S.Admin imports SCD while S.Sigy is currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "yes" after import of the SCD as a single operation

#### FMT\_MTD.1/Admin Management of TSF data

**FMT\_MTD.1.1/Admin [Editorially Refined]** The TSF shall restrict the ability to **create** the **RAD** to **R.Admin**.

#### FMT\_MTD.1/Signatory Management of TSF data

**FMT\_MTD.1.1/Signatory** The TSF shall restrict the ability to **modify and none** the **RAD** to **R.Sigy**.

##### 9.1.1.3 Identification and authentication (FIA)

#### FIA\_UID.1 Timing of identification

**FIA\_UID.1.1** The TSF shall allow

- **Self-test according to FPT\_TST.1,**
- **Establishing a trusted channel between a trusted IT product generating the SCD/SVD pair for import of the SCD as described by FDP\_UCT.1/SCD and FDP\_ITC.1/SCD and the TOE by means of TSF required by FTP\_ITC.1/SCD (not applicable for SSCD KG).**
- **Establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP\_ITC.1/SVD to export the SVD to the CGA ([PP-SSCD4]).**
- **Establishing a trusted channel between the HID and the TOE by means of TSF required by FTP\_ITC.1/VAD to send the VAD ([PP-SSCD5], [PP-SSCD6]).**
- **Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP\_ITC.1/DTBS to send the DTBS ([PP-SSCD5], [PP-SSCD6])**

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

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

## FIA\_AFL.1 Authentication failure handling

**FIA\_AFL.1.1** The TSF shall detect when **an administrator configurable positive integer within [1 and 127]** unsuccessful authentication attempts occur related to **consecutive failed authentication attempts**.

**FIA\_AFL.1.2** When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **Block RAD**.

## FIA\_UAU.1 Timing of authentication

**FIA\_UAU.1.1** The TSF shall allow

- o **Self-test according to FPT\_TST.1,**
- o **Identification of the user by means of TSF required by FIA\_UID.1**
- o **Establishing a trusted channel between a trusted IT product generating the SCD/SVD pair for import the SCD as described by FDP\_UCT.1/SCD and FDP\_ITC.1/SCD and the TOE by means of TSF required by FTP\_ITC.1/SCD (not applicable for SSCD KG).**
- o **Establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP\_ITC.1/SVD to export the SVD to the CGA ([PP-SSCD4]).**
- o **Establishing a trusted channel between the HID and the TOE by means of TSF required by FTP\_ITC.1/VAD to send the VAD ([PP-SSCD5], [PP-SSCD6]).**
- o **Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP\_ITC.1/DTBS to send the DTBS ([PP-SSCD5], [PP-SSCD6])**

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

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

### 9.1.1.4 User data protection (FDP)

The security attributes and related status for the subjects and objects are:

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	authorised, not authorised
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value

**FDP\_SDI.2/DTBS Stored data integrity monitoring and action**

**FDP\_SDI.2.1/DTBS** The TSF shall monitor user data stored in containers controlled by the TSF for **integrity error** on all objects, based on the following attributes: **integrity checked stored DTBS**.

**FDP\_SDI.2.2/DTBS** Upon detection of a data integrity error, the TSF shall

- o **prohibit the use of the altered data**
- o **inform the S.Sigy about integrity error.**

**FDP\_SDI.2/Persistent Stored data integrity monitoring and action**

**FDP\_SDI.2.1/Persistent** The TSF shall monitor user data stored in containers controlled by the TSF for **integrity error** on all objects, based on the following attributes: **integrity checked stored data**.

**FDP\_SDI.2.2/Persistent** Upon detection of a data integrity error, the TSF shall

- o **prohibit the use of the altered data**
- o **inform the S.Sigy about integrity error.**

**FDP\_RIP.1 Subset residual information protection**

**FDP\_RIP.1.1** The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects:

- o **Session keys (PACE-KMAC, PACE-KEnc), (CA-KMAC, CA-KEnc) (immediately after closing related communication session),**
- o **the ephemeral private key ephem - SKPICC- PACE (by having generated a DH shared secret K),**
- o **secret electronic document holder authentication data, e.g. PIN and/or PUK (when their temporarily stored values are not used any more),**
- o **The following data persistently stored by the TOE shall have the user data attribute "integrity checked persistent stored data":**
  - o **SCD**
  - o **SVD (if persistently stored by the TOE)**
- o **The following data temporarily stored by the TOE shall have the user data attribute "integrity checked stored data":**
  - o **DTBS/R.**

*Application Note:*

This SFR covers the definition in SSCD PPs and extends them by session keys, keys and PIN/PUK as part of the EAC V2 protocol aspects. This extension does not conflict with the strict conformance to SSCD PPs.

**FDP\_ACC.1/Signature\_Creation Subset access control**

**FDP\_ACC.1.1/Signature\_Creation** The TSF shall enforce the **Signature Creation SFP** on **Sending of DTBS/R by SCA and Signing of DTBS/R by Signatory**:

- o **subjects: S.User,**
- o **objects: DTBS/R, SCD,**
- o **operations: signature creation.**

**FDP\_ACF.1/Signature\_Creation Security attribute based access control**

**FDP\_ACF.1.1/Signature\_Creation** The TSF shall enforce the **Signature Creation SFP** to objects based on the following:

- o **the user S.User is associated with the security attribute "Role" and**
- o **the SCD with the security attribute "SCD Operational".**

**FDP\_ACF.1.2/Signature\_Creation** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **R.Sigy is allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes".**

**FDP\_ACF.1.3/Signature\_Creation** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

**FDP\_ACF.1.4/Signature\_Creation** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no".**

**9.1.1.5 Cryptographic support (FCS)****FCS\_COP.1 Cryptographic operation**

**FCS\_COP.1.1** The TSF shall perform [**Cryptographic Operation**] in accordance with a specified cryptographic algorithm [**Algorithms**] and cryptographic key sizes [**Key sizes**] that meet the following: [**Standards**]

Cryptographic Operation	Algorithms	Key sizes	Standards
Digital signature computation	RSA PKCS#1v1.5, RSA-PSS PKCS#1 v2.1, with SHA-1 SHA-224 SHA-256 SHA-384 or SHA-512	1024, 1536, 2048, 2560, 3072 and 4096	RSA PKCS1 v2.1
Digital signature computation	ECDSA with SHA-1 SHA-224 SHA-256 SHA-384 or SHA-512	256, 320, 384, 512, 521 bits	Signature Creation: ANSI_X9.62-2005, Public key cryptography for the financial services Industry: The elliptic curve digital signature algorithm (ECDSA), ANSI, 2005-11-16, section 7.3
Key agreement	ECDH	192,224,256,320,384,512 and 521	419212-1
Mutual authentication for secure messaging	3DES CBC EDE 128 bits (encipherment) + Retail MAC with SHA-1, SHA-256	128 bits	Addendum IAS-ECC v1.0.1
Mutual authentication for secure messaging	AES with SHA-256	128, 192, 256 bits	Addendum IAS-ECC v1.0.1
PACE Authentication	PACE IM and GM with ECDH, DES, AES	ECDH: 192,224,256, 320,384, 512, 521 bits AES: 128 192 256, DES:128	ICAO Technical Report-Supplemental Access Control for Machine Readable Travel Documents Release: 1.01 November 2010
Secure messaging - Encryption/decryption	3DES in CBC mode or AES in CBC mode	3DES: 128 bits, AES:128, 192, 256 bits	Addendum IAS-ECC v1.0.1



secure messaging - MAC generation and verification	ISO/IEC 9797-1 algorithm 3 padding 2 (3DES) or CMAC (AES)	3DES: 128 bits, AES: 128, 192, 256 bits	DES: ISO9797 - AES: NIST SP 800-38B
Hash calculation within the digital signature sequence	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	none	NIST FIPS PUB 180-2
Cipherring key encryption	RSA PKCS#1v1.5	1024, 1536, 2048, 2560, 3072, and 4096 bits	RSA PKCS1 v2.1
Cipherring key decryption	RSA-OAEP, PKCS#1 v2.1, RSA PKCS#1v1.5	1024, 1536, 2048, 2560, 3072, and 4096 bits	RSA PKCS1 v2.1

### FCS\_CKM.4 Cryptographic key destruction

**FCS\_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **physically overwriting the keys in a randomized manner** that meets the following: **none**.

#### 9.1.2 SSCD parts 2, 4 and 5 only

##### 9.1.2.1 Cryptographic support (FCS)

### FCS\_CKM.1 Cryptographic key generation

**FCS\_CKM.1.1** The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm [**Cryptographic key generation algorithm**] and specified cryptographic key sizes [**Cryptographic key sizes**] that meet the following: [**Standards**]

Cryptographic key generation algorithm	Cryptographic key sizes	Standards
EC key pair generation	192,224,256, 320,384, 512 and 521 bits	ANS X9.62
RSA CRT Key pair generation	1024, 1536, 2048, 2560, 3072 and 4096 bits	RSA PKCS#1 v2.1

##### 9.1.2.2 User data protection (FDP)

The security attributes and related status for the subjects and objects are:

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	authorised, not authorised
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value

### FDP\_ACC.1/SVD\_Transfer Subset access control

**FDP\_ACC.1.1/SVD\_Transfer** The TSF shall enforce the **SVD Transfer SFP** on

- o **subjects: S.User,**
- o **objects: SVD,**
- o **operations: export.**

### FDP\_ACF.1/SVD\_Transfer Security attribute based access control

**FDP\_ACF.1.1/SVD\_Transfer** The TSF shall enforce the **SVD Transfer SFP** to objects based on the following:

- o **the S.User is associated with the security attribute Role,**
- o **the SVD.**

**FDP\_ACF.1.2/SVD\_Transfer** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **R.Admin and R.Sigy is allowed to export SVD.**

**FDP\_ACF.1.3/SVD\_Transfer** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

**FDP\_ACF.1.4/SVD\_Transfer** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none.**

### FDP\_ACC.1/SCD/SVD\_Generation Subset access control

**FDP\_ACC.1.1/SCD/SVD\_Generation** The TSF shall enforce the **SCD/SVD Generation SFP** on

- o **subjects: S.User,**
- o **objects: SCD, SVD,**
- o **operations: generation of SCD/SVD pair.**

**FDP\_ACF.1/SCD/SVD\_Generation Security attribute based access control**

**FDP\_ACF.1.1/SCD/SVD\_Generation** The TSF shall enforce the **SCD/SVD Generation SFP** to objects based on the following: **the user S.User is associated with the security attribute "SCD/SVD Management"**.

**FDP\_ACF.1.2/SCD/SVD\_Generation** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **S.User with the security attribute "SCD/SVD Management" set to "authorised" is allowed to generate SCD/SVD pair.**

**FDP\_ACF.1.3/SCD/SVD\_Generation** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

**FDP\_ACF.1.4/SCD/SVD\_Generation** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.**

**9.1.3 SSCD parts 3 and 6 only****9.1.3.1 Trusted path/channels (FTP)****FTP\_ITC.1/SCD Inter-TSF trusted channel**

**FTP\_ITC.1.1/SCD** The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP\_ITC.1.2/SCD** The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

**FTP\_ITC.1.3/SCD** The TSF shall initiate communication via the trusted channel for

- o **Data exchange integrity according to FDP\_UCT.1/SCD.**

**9.1.3.2 User data protection (FDP)**

The security attributes and related status for the subjects and objects are:

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	authorised, not authorised
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value

### FDP\_UCT.1/SCD Basic data exchange confidentiality

**FDP\_UCT.1.1/SCD [Editorially Refined]** The TSF shall enforce the **SCD Import SFP** to **receive SCD** in a manner protected from unauthorised disclosure.

### FDP\_ITC.1/SCD Import of user data without security attributes

**FDP\_ITC.1.1/SCD** The TSF shall enforce the **SCD Import SFP** when importing user data, controlled under the SFP, from outside of the TOE.

**FDP\_ITC.1.2/SCD [Editorially Refined]** The TSF shall ignore any security attributes associated with the **SCD** when imported from outside the TOE.

**FDP\_ITC.1.3/SCD** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **The SCD shall be sent by an authorized trusted IT environment.**

### FDP\_ACC.1/SCD\_Import Subset access control

**FDP\_ACC.1.1/SCD\_Import** The TSF shall enforce the **SCD Import SFP** on

- o **subjects: S.User,**
- o **objects: SCD,**
- o **operations: import of SCD.**

**FDP\_ACF.1/SCD\_Import Security attribute based access control**

**FDP\_ACF.1.1/SCD\_Import** The TSF shall enforce the **SCD Import SFP** to objects based on the following: **the user S.User is associated with the security attribute "SCD/SVD Management"**.

**FDP\_ACF.1.2/SCD\_Import** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **S.User with the security attribute "SCD/SVD Management" set to "authorised" is allowed to import SCD.**

**FDP\_ACF.1.3/SCD\_Import** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

**FDP\_ACF.1.4/SCD\_Import** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to import SCD.**

**9.1.4 SSSCD part 4 only****9.1.4.1 Trusted path/channels (FTP)****FTP\_ITC.1/SVD Inter-TSF trusted channel**

**FTP\_ITC.1.1/SVD [Editorially Refined]** The TSF shall provide a communication channel between itself and another trusted IT product **CGA** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP\_ITC.1.2/SVD [Editorially Refined]** The TSF shall permit **the CGA** to initiate communication via the trusted channel.

**FTP\_ITC.1.3/SVD [Editorially Refined]** The TSF **or the CGA shall** initiate communication via the trusted channel for

- o **data Authentication with Identity of Guarantor according to FIA\_API.1 and FDP\_DAU.2/SVD.**

	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>94/142</b>
---	--	--

#### 9.1.4.2 User data protection (FDP)

### FDP\_DAU.2/SVD Data Authentication with Identity of Guarantor

**FDP\_DAU.2.1/SVD** The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **SVD**.

**FDP\_DAU.2.2/SVD** The TSF shall provide **CGA** with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

#### 9.1.4.3 Identification and authentication (FIA)

### FIA\_API.1 Authentication Proof of Identity

**FIA\_API.1.1** The TSF shall provide a

- o **Mutual Authentication according to [IAS ADD]**
- o **PACE Authentication according to [ICA09303]**

to prove the identity of the **SSCD**.

#### 9.1.5 SSCD parts 5 and 6 only

##### 9.1.5.1 User data protection (FDP)

### FDP\_UIT.1/DTBS Data exchange integrity

**FDP\_UIT.1.1/DTBS** The TSF shall enforce the **Signature Creation SFP** to **receive** user data in a manner protected from **modification and insertion** errors.

**FDP\_UIT.1.2/DTBS** The TSF shall be able to determine on receipt of user data, whether **modification and insertion** has occurred.

##### 9.1.5.2 Trusted path/channels (FTP)

### FTP\_ITC.1/VAD Inter-TSF trusted channel

**FTP\_ITC.1.1/VAD [Editorially Refined]** The TSF shall provide a communication channel between itself and another trusted IT product **HID** that is logically distinct from other

communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP\_ITC.1.2/VAD [Editorially Refined]** The TSF shall permit **the HID** to initiate communication via the trusted channel.

**FTP\_ITC.1.3/VAD [Editorially Refined]** The TSF **or the HID** shall initiate communication via the trusted channel for:

- o **User authentication according to FIA\_UAU.1**

#### **FTP\_ITC.1/DTBS Inter-TSF trusted channel**

**FTP\_ITC.1.1/DTBS [Editorially Refined]** The TSF shall provide a communication channel between itself and another trusted IT product **SCA** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP\_ITC.1.2/DTBS [Editorially Refined]** The TSF shall permit **the SCA** to initiate communication via the trusted channel.

**FTP\_ITC.1.3/DTBS [Editorially Refined]** The TSF **or the SCA** shall initiate communication via the trusted channel for **signature creation**.

#### **9.1.6 Additional SFRs related to EAC2**

#### **FCS\_RND.1 Quality metric for random numbers**

**FCS\_RND.1.1** The TSF shall provide a mechanism to generate random numbers that meet **FCS\_RNG.1 Quality metric for random numbers of [ST-PL]**.

#### **FCS\_CKM.1/DH\_PACE Cryptographic key generation**

**FCS\_CKM.1.1/DH\_PACE** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH compliant to [TR03111]** and specified cryptographic key sizes **192, 224, 256 and 320, 384, 512, and 521 bits in combination with 112 bits 3DES or 128, 192 or 256 bits AES** that meet the following: **[TR03110-2]**.

### FCS\_COP.1/SHA Cryptographic operation

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

### FCS\_COP.1/SIG\_VER Cryptographic operation

**FCS\_COP.1.1/SIG\_VER** The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **ECDSA** and cryptographic key sizes **160, 192, 224, 256, 320, 384, 512 and 521 bits** that meet the following: **ISO15946-2 specified in [ISO15946-2], in combination with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 digest algorithms.**

*Application Note:*

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

### FCS\_COP.1/PACE\_ENC Cryptographic operation

**FCS\_COP.1.1/PACE\_ENC** The TSF shall perform **[Cryptographic Operation]** in accordance with a specified cryptographic algorithm **[Algorithms]** and cryptographic key sizes **[Key sizes]** that meet the following: **[Standards]**

Cryptographic Operation	Algorithms	Key sizes	Standards
secure messaging-encryption and decryption	AES in CBC mode	128, 192 and 256 bits	[TR-03110-3]
secure messaging-encryption and decryption	TDES in CBC mode	112 bits	[IAS-ECC]

### FCS\_COP.1/PACE\_MAC Cryptographic operation

**FCS\_COP.1.1/PACE\_MAC** The TSF shall perform **[Cryptographic Operation]** in accordance with a specified cryptographic algorithm **[Algorithms]** and cryptographic key sizes **[Key sizes]** that meet the following: **[Standards]**

Cryptographic Operation	Algorithms	Key sizes	Standards
secure messaging - message authentication code	CMAC	128, 192 and 256 bits	[TR03110-2]
secure messaging - message authentication code	Retail-MAC	112 bits	[TR03110-2]



**FIA\_UAU.1/PACE Timing of authentication**

**FIA\_UAU.1.1/PACE [Editorially Refined]** The TSF shall allow

- o **To establish a communication channel,**
- o **Carrying out the PACE (PIN, PUK, MRZ or CAN) protocol according to [TR03110-2],**
- o **To read the Initialization Data if it is not disabled by TSF according to FMT\_MTD.1/INI\_DIS,**

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

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

**FIA\_UAU.5/PACE Multiple authentication mechanisms**

**FIA\_UAU.5.1/PACE [Editorially Refined]** The TSF shall provide

- o **PACE (PIN, PUK, MRZ or CAN) protocol according to [TR03110-2],**
- o **Secure Messaging according to [TR03110-3],**
- o **Symmetric Authentication Mechanism based on AES or TDES,**
- o **Terminal Authentication 2 protocol according to [TR03110-2],**
- o **Chip Authentication 2 according to [TR03110-2]**

to support user authentication.

**FIA\_UAU.5.2/PACE [Editorially Refined]** The TSF shall authenticate any user's claimed identity according to the **following rules:**

- o **Having successfully run the PACE (PIN, PUK, MRZ or CAN) protocol the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by the PACE protocol.**
- o **The TOE accepts the authentication attempt by means of the Terminal Authentication 2 protocol, only if (i) the terminal presents its static public key PKPCD and the key is successfully verifiable up to the CVCA and (ii) the terminal uses the PICC identifier IDPICC = Comp (ephem-PKPICC-PACE) calculated during, and the secure messaging established by the current PACE (PIN, PUK, MRZ or CAN) authentication.**
- o **Having successfully run Chip Authentication 2, the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by Chip Authentication 2.**

**FIA\_AFL.1/Suspend\_PIN Authentication failure handling**

**FIA\_AFL.1.1/Suspend\_PIN [Editorially Refined]** The TSF shall detect when **an administrator configurable positive integer within 1 byte** unsuccessful authentication attempts occur related to **consecutive failed authentication attempts using the PIN or PUK as the shared password for PACE.**

**FIA\_AFL.1.2/Suspend\_PIN [Editorially Refined]** When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **suspend the reference value of the PIN or PUK according to [TR03110-2].**

**FIA\_AFL.1/Block\_PIN Authentication failure handling**

**FIA\_AFL.1.1/Block\_PIN [Editorially Refined]** The TSF shall detect when **an administrator configurable positive integer within 1 byte** unsuccessful authentication attempts occur related to **consecutive failed authentication attempts using the suspended PIN or PUK as the shared password for PACE.**

**FIA\_AFL.1.2/Block\_PIN [Editorially Refined]** When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **block the reference value of PIN or PUK according to [TR03110-2].**

**FIA\_AFL.1/PACE Authentication failure handling**

**FIA\_AFL.1.1/PACE [Editorially Refined]** The TSF shall detect when **an administrator configurable positive integer within 1 byte** unsuccessful authentication attempts occur related to **authentication attempts using the PIN, PUK, MRZ or CAN password as the shared password for PACE.**

**FIA\_AFL.1.2/PACE** When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **delay each of the following authentication attempts until the next successful authentication attempt by an configurable amount of time.**

**FIA\_UAU.1/EAC2\_Terminal Timing of authentication**

**FIA\_UAU.1.1/EAC2\_Terminal [Editorially Refined]** The TSF shall allow

- **To establish a communication channel,**
- **Carrying out the PACE (PIN, PUK, MRZ or CAN) protocol according to [TR03110-2],**
- **To read the Initialization Data if it is not disabled by TSF according to FMT\_MTD.1/INI\_DIS,**
- **Carrying out the Terminal Authentication protocol 2 according to [TR03110-2]**

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

**FIA\_UAU.1.2/EAC2\_Terminal** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

#### **FIA\_API.1/CA Authentication Proof of Identity**

**FIA\_API.1.1/CA** The TSF shall provide a **protocol Chip Authentication 2 according to [TR03110-2]** to prove the identity of the **TOE**.

#### **FIA\_UAU.6/CA Re-authenticating**

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

#### **FIA\_UID.1/PACE Timing of identification**

**FIA\_UID.1.1/PACE [Editorially Refined]** The TSF shall allow

- o **To establish a communication channel,**
- o **Carrying out the PACE (PIN, PUK, MRZ or CAN) protocol according to [TR03110-2],**
- o **To read the Initialization Data if it is not disabled by TSF according to FMT\_MTD.1/INI\_DIS**

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

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

#### **FIA\_UID.1/EAC2\_Terminal Timing of identification**

**FIA\_UID.1.1/EAC2\_Terminal [Editorially Refined]** The TSF shall allow

- o **To establish a communication channel,**
- o **Carrying out the PACE (PIN, PUK, MRZ or CAN) protocol according to [TR03110-2],**
- o **To read the Initialization Data if it is not disabled by TSF according to FMT\_MTD.1/INI\_DIS,**
- o **Carrying out the Terminal Authentication protocol 2 according to [TR03110-2]**

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

**FIA\_UID.1.2/EAC2\_Terminal** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

**FIA\_UAU.4/PACE Single-use authentication mechanisms**

**FIA\_UAU.4.1/PACE [Editorially Refined]** The TSF shall prevent reuse of authentication data related to

- o **PACE (PIN, PUK, MRZ or CAN) protocol according to [TR03110-2],**
- o **Terminal Authentication 2 protocol according to [TR03110-2].**

**FIA\_UAU.6/PACE Re-authenticating**

**FIA\_UAU.6.1/PACE** The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal.**

**FDP\_ACC.1/TRM Subset access control**

**FDP\_ACC.1.1/TRM** The TSF shall enforce the **Access Control SFP** on **terminals gaining access User data stored in the TOE (including sensitive user data) and selected by the personalization agent, and all TOE intrinsic secret (i.e. cryptographic) data.**

**FDP\_ACF.1/TRM Security attribute based access control**

**FDP\_ACF.1.1/TRM** The TSF shall enforce the **Access Control SFP** to objects based on the following:

- o **Subjects: Terminal, PACE terminal, EAC2 terminal.**
- o **Objects:**
  - a. **User data stored in the TOE (including sensitive user data) and selected by the personalization agent,**
  - b. **all TOE intrinsic secret (i.e. cryptographic) data.**
- o **Security attributes: Terminal Authorization Level (access rights).**

**FDP\_ACF.1.2/TRM** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **A PACE terminal is allowed to read data objects data (object 2.a) specified in FDP\_ACF.1.1/TRM after successful PACE authentication according to [TR03110-2], as required by FIA\_UAU.1/PACE.**

**FDP\_ACF.1.3/TRM** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

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

- o **Any terminal not being a PACE terminal or an EAC2 terminal is not allowed to read, to write, to modify, or to use any user data (object 2.a) specified in FDP\_ACF.1.1/TRM.**

- Terminals not using secure messaging are not allowed to read, write, modify, or use any user data (object 2.a) specified in FDP\_ACF.1.1/TRM.
- Reading, modifying, writing, or using sensitive user data protected by TAV2 and CAV2 (object 2.a specified in FDP\_ACF.1.1/TRM) is only allowed to EAC2 terminals using the following mechanism: The TOE applies the EAC2 protocol (cf. FIA\_UAU.5) to determine access rights of the terminal according to [TR03110-2]. To determine the effective authorization of a terminal, the chip must calculate a bitwise Boolean 'and' of the relative authorization contained in the CHAT and Extended CHAT of the Terminal Certificate, the referenced DV Certificate, and the referenced CVCA Certificate. Based on the terminal type drawn from the CHAT and Extended CHAT of the Terminal Certificate, the TOE shall grant the right to read, modify or write sensitive user data, or perform operations using these sensitive user data.
- No subject is allowed to read, write, modify, or use the data objects TOE intrinsic secrets (object 2.b) specified in FDP\_ACF.1.1/TRM.

#### FDP\_UCT.1/TRM Basic data exchange confidentiality

**FDP\_UCT.1.1/TRM** The TSF shall enforce the **Access Control SFP** to **transmit** user data in a manner protected from unauthorised disclosure.

#### FDP\_UIT.1/TRM Data exchange integrity

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

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

#### FTP\_ITC.1/PACE Inter-TSF trusted channel

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

**FTP\_ITC.1.2/PACE [Editorially Refined]** The TSF shall permit a **PACE terminal** to initiate communication via the trusted channel.

**FTP\_ITC.1.3/PACE** The TSF shall initiate communication via the trusted channel for **any data exchange between the TOE and a PACE terminal after PACE.**

**FMT\_SMR.1/PACE Security roles**

**FMT\_SMR.1.1/PACE** The TSF shall maintain the roles

- o **Manufacturer,**
- o **Personalization Agent,**
- o **Terminal,**
- o **PACE terminal,**
- o **Country Verifying Certification Authority,**
- o **Document Verifier,**
- o **EAC2 terminal,**
- o **Electronic document holder.**

**FMT\_SMR.1.2/PACE** The TSF shall be able to associate users with roles.

**FMT\_MTD.1/CVCA\_INI Management of TSF data**

**FMT\_MTD.1.1/CVCA\_INI** The TSF shall restrict the ability to **write** the

- o **Initial CVCA Public Key,**
- o **meta-data of the initial CVCA Certificate as required in [TR03110-2], resp [TR03110-3]**
- o **initial Current Date**

to **the personalization agent.**

**FMT\_MTD.1/CVCA\_UPD Management of TSF data**

**FMT\_MTD.1.1/CVCA\_UPD** The TSF shall restrict the ability to **update** the

- o **CVCA Public Key (PKCVCA),**
- o **meta-data of the CVCA Certificate as required by [TR03110-2], resp [TR03110-3]**

to **the Country Verifying Certification Authority.**

**FMT\_MTD.1/DATE Management of TSF data**

**FMT\_MTD.1.1/DATE** The TSF shall restrict the ability to **modify** the **the current date** to

- o **CVCA,**
- o **Document Verifier,**
- o **EAC2 terminal possessing an Accurate Terminal Certificate according to [TR03110-3].**

**FMT\_MTD.1/PA Management of TSF data**

**FMT\_MTD.1.1/PA** The TSF shall restrict the ability to **write** the **card/chip security object(s) (SOC)** selected in **Access Control SFP** and the document **Security Object (SOD)** selected in **Access Control SFP** to **the Personalization Agent**.

**FMT\_MTD.1/SK\_PICC Management of TSF data**

**FMT\_MTD.1.1/SK\_PICC** The TSF shall restrict the ability to **load** the **Chip Authentication private key(s) (SKPICC)** selected in **Access Control SFP** to **the personalization agent**.

**FMT\_MTD.1/KEY\_READ Management of TSF data**

**FMT\_MTD.1.1/KEY\_READ** The TSF shall restrict the ability to **read** the

- o **PACE passwords,**
- o **The Chip Authentication private key(s) (SKPICC)**

to **none**.

**FMT\_MTD.1/Initialize\_PIN Management of TSF data**

**FMT\_MTD.1.1/Initialize\_PIN** The TSF shall restrict the ability to **write** the **PIN, PUK, MRZ and CAN,** selected in **Access Control SFP** to **the personalization agent**.

**FMT\_MTD.1/Resume\_PIN Management of TSF data**

**FMT\_MTD.1.1/Resume\_PIN** The TSF shall restrict the ability to **resume** the **suspended PIN** selected in **Access Control SFP** to **the electronic document holder (Signatory)**.

**FMT\_MTD.1/Change\_PIN Management of TSF data**

**FMT\_MTD.1.1/Change\_PIN** The TSF shall restrict the ability to **change** the **blocked PIN** selected in **Access Control SFP** to

- o **The electronic document holder (using the Current PUK for changing),**
- o **An authorized terminal that has access to change the current PIN.**

**FMT\_MTD.1/Unblock\_PIN Management of TSF data**

**FMT\_MTD.1.1/Unblock\_PIN** The TSF shall restrict the ability to **unblock** the **blocked PIN (including a blocked RAD) selected in Access Control SFP** to

- o **the electronic document holder (using the PUK for unblocking),**
- o **An authorized terminal that has access to unblock the current PIN.**

**FMT\_MTD.3 Secure TSF data**

**FMT\_MTD.3.1** The TSF shall ensure that only secure values are accepted for **TSF data of the Terminal Authentication protocol 2 and the Access Control SFP.**

**FMT\_MTD.1/INI\_ENA Management of TSF data**

**FMT\_MTD.1.1/INI\_ENA** The TSF shall restrict the ability to **write** the **Initialisation Data and the Pre-personalisation Data** to **the Manufacturer.**

**FMT\_MTD.1/INI\_DIS Management of TSF data**

**FMT\_MTD.1.1/INI\_DIS** The TSF shall restrict the ability to **read out** the **Initialisation Data and the Pre-personalisation Data** to **the Personalisation Agent.**

**FTP\_ITC.1/CA2 Inter-TSF trusted channel**

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

**FTP\_ITC.1.2/CA2 [Editorially Refined]** The TSF shall permit **an EAC2 terminal** to initiate communication via the trusted channel.

**FTP\_ITC.1.3/CA2** The TSF shall initiate communication via the trusted channel for **any data exchange between the TOE and an EAC2 terminal after Chip Authentication 2.**



**FMT\_LIM.1 Limited capabilities**

**FMT\_LIM.1.1** The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT\_LIM.2)' the following policy is enforced

**Deploying test features after TOE delivery do not allow**

- o **User Data to be manipulated and disclosed,**
- o **TSF data to be manipulated or disclosed,**
- o **software to be reconstructed,**
- o **substantial information about construction of TSF to be gathered which may enable other attacks**

**FMT\_LIM.2 Limited capabilities**

**FMT\_LIM.2.1** The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT\_LIM.1)' the following policy is enforced

**Deploying test features after TOE delivery do not allow**

- o **User Data to be manipulated and disclosed,**
- o **TSF data to be manipulated or disclosed,**
- o **software to be reconstructed,**
- o **substantial information about construction of TSF to be gathered which may enable other attacks**

## 9.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL5 augmented with AVA\_VAN.5 and ALC\_DVS.2.

	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>106/142</b>
---	--	---

## 9.3 Security Requirements Rationale

### 9.3.1 Objectives

#### 9.3.1.1 Security Objectives for the TOE

##### All SSCD parts

**OT.Tamper\_Resistance** is provided by FPT\_PHP.3 to resist physical attacks.

**OT.Tamper\_ID** is provided by FPT\_PHP.1 by the means of passive detection of physical attacks.

**OT.EMSEC\_Design** covers that no intelligible information is emanated. This is provided by FPT\_EMS.1.1.

**OT.DTBS\_Integrity\_TOE** ensures that the DTBS/R is not altered by the TOE. The integrity functions specified by FDP\_SDI.2/DTBS require that the DTBS/R has not been altered by the TOE.

**OT.Sigy\_SigF** is provided by an SFR for identification authentication and access control.

FIA\_UAU.1 and FIA\_UID.1 ensure that no signature creation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT\_MTD.1/Admin and FMT\_MTD.1/Signatory manage the authentication function. SFR FIA\_AFL.1 provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP\_SDI.2/DTBS ensures the integrity of stored DTBS and FDP\_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process).

The security functions specified by FDP\_ACC.1/Signature\_Creation and FDP\_ACF.1/Signature\_Creation provide access control based on the security attributes managed according to the SFR FMT\_MTD.1/Signatory, FMT\_MSA.2, FMT\_MSA.3 and FMT\_MSA.4. The SFR FMT\_SMF.1 and FMT\_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory. FMT\_MOF.1 restricts the ability to enable the signature creation function to the signatory. FMT\_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.

**OT.Sig\_Secure** is provided by the cryptographic algorithms specified by FCS\_COP.1, which ensures the cryptographic robustness of the signature algorithms. FDP\_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE and FPT\_TST.1 ensures self-tests ensuring correct signature creation.

**OT.SCD\_Secrecy** is provided by the security functions specified by the following SFR. FCS\_CKM.1 ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. The security functions specified by FDP\_RIP.1 and

FCS\_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been used for signature creation and that destruction of SCD leaves no residual information.

The security functions specified by FDP\_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT\_TST.1 tests the working conditions of the TOE and FPT\_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT\_FLS.1 is fault injection for differential fault analysis (DFA). FDP\_UCT.1/SCD and FTP\_ITC.1/SCD ensures the confidentiality for SCD import. SFR FPT\_EMS.1 and FPT\_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

**OT.Lifecycle\_Security** is provided by the SFR for SCD/SVD generation FCS\_CKM.1, SCD usage FCS\_COP.1 and SCD destruction FCS\_CKM.4 which ensure cryptographically secure lifecycle of the SCD. The SCD/SVD generation is controlled by TSF according to FDP\_ACC.1/SCD/SVD\_Generation and FDP\_ACF.1/SCD/SVD\_Generation. The SVD transfer for certificate generation is controlled by TSF according to FDP\_ACC.1/SVD\_Transfer and FDP\_ACF.1/SVD\_Transfer. The SCD usage is ensured by access control FDP\_ACC.1/Signature\_Creation, FDP\_ACF.1/Signature\_Creation which is based on the security attribute secure TSF management according to FMT\_MOF.1, FMT\_MSA.1/Admin, FMT\_MSA.1/Signatory, FMT\_MSA.2, FMT\_MSA.3, FMT\_MSA.4, FMT\_MTD.1/Admin, FMT\_MTD.1/Signatory, FMT\_MTD.1/Unblock\_PIN, FMT\_SMF.1 and FMT\_SMR.1. The test functions FPT\_TST.1 provides failure detection throughout the lifecycle. The SCD import is controlled by TSF according to FDP\_ACC.1/SCD\_Import, FDP\_ACF.1/SCD\_Import and FDP\_ITC.1/SCD. The confidentiality of the SCD is protected during import according to FDP\_UCT.1/SCD in the trusted channel FTP\_ITC.1/SCD.

#### SSCD parts 2, 4 and 5 only

**OT.SCD\_SVD\_Corresp** addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS\_CKM.1 to generate corresponding SVD/SCD pairs. The security functions specified by FDP\_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Moreover, the SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. The management functions identified by FMT\_SMF.1 and by FMT\_MSA.4 allow R.Admin to modify the default value of the security attribute SCD Identifier.

**OT.SCD\_Unique** implements the requirement of practically unique SCD as laid down in Annex III [DIR], paragraph 1(a), which is provided by the cryptographic algorithms specified by FCS\_CKM.1.

**OT.SCD/SVD\_Gen** addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by FIA\_UID.1 and FIA\_UAU.1 provide user identification and user authentication prior to enabling access to authorised functions. The SFR FDP\_ACC.1/SCD/SVD\_Generation and FDP\_ACF.1/SCD/SVD\_Generation provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by FMT\_MSA.1/Admin, FMT\_MSA.2, and FMT\_MSA.3 for static attribute

	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>108/142</b>
---	--	---

initialisation. The SFR FMT\_MSA.4 defines rules for inheritance of the security attribute 'SCD operational' of the SCD.

**SSCD parts 3 and 6 only**

**OT.SCD\_Auth\_Imp** is provided by the security functions specified by the following SFR. FIA\_UID.1 and FIA\_UAU.1 ensure that the user is identified and authenticated before SCD can be imported. FDP\_ACC.1/SCD\_Import and FDP\_ACF.1/SCD\_Import ensure that only authorised users can import SCD.

**SSCD part 4 only**

**OT.TOE\_SSCD\_Auth** requires the TOE to provide security mechanisms to identify and to authenticate themselves as SSCD, which is directly provided by FIA\_API.1 (Authentication Proof of Identity). The SFR FIA\_UAU.1 allows (additionally to the core PP Part2 SSCD KG) establishment of the trusted channel before (human) user is authenticated.

**OT.TOE\_TC\_SVD\_Exp** requires the TOE to provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA, which is directly provided by

- o The SVD transfer for certificate generation is controlled by TSF according to FDP\_ACC.1/SVD\_Transfer and FDP\_ACF.1/SVD\_Transfer.
- o FDP\_DAU.2/SVD (Data Authentication with Identity of Guarantor), which requires the TOE to provide CGA with the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence.
- o FTP\_ITC.1/SVD Inter-TSF trusted channel), which requires the TOE to provide a trusted channel to the CGA.

**SSCD parts 5 and 6 only**

**OT.TOE\_TC\_VAD\_Imp** is provided by FTP\_ITC.1/VAD to provide a trusted channel to protect the VAD provided by the HID to the TOE.

**OT.TOE\_TC\_DTBS\_Imp** is provided by FTP\_ITC.1/DTBS to provide a trusted channel to protect the DTBS provided by the SCA to the TOE and by FDP\_UIT.1/DTBS, which requires the TSF to verify the integrity of the received DTBS.

**Security Objectives OT related to EAC2**

**OT.AC\_Pers\_EAC2** The security objective OT.AC\_Pers\_EAC2 ensures that only the personalization agent can write user- and TSF-Data into the TOE, and that some of this data cannot be altered after personalization. This property is covered by FDP\_ACC.1/TRM and FDP\_ACF.1/TRM requiring, amongst other, an appropriate authorization level of an EAC2 terminal. This authorization level can be achieved by terminal identification/authentication as required by the SFRs FIA\_UID.1/EAC2\_Terminal and FIA\_UAU.1/EAC2\_Terminal. The SFRs FMT\_SMF.1 and FMT\_SMR.1/PACE support the related functions and roles. Since only an EAC2 terminal can reach the necessary authorization level, using and managing the PIN (the related SFRs are FIA\_AFL.1/Suspend\_PIN, FIA\_AFL.1/Block\_PIN, FMT\_MTD.1/Resume\_PIN,

FMT\_MTD.1/Change\_PIN, FMT\_MTD.1/Unblock\_PIN, and FMT\_MTD.1/Initialize\_PIN) also support the achievement of this objective. FDP\_RIP.1 requires erasing the temporal values PIN and PUK. The justification for the SFRs FMT\_MTD.1/INI\_ENA and FMT\_MTD.1/INI\_DIS arises from the justification for OT.Identification above with respect to the pre-personalization data. FMT\_MTD.1/PA covers the related property of OT.AC\_Pers\_EAC2 (writing/updating SOC and SOD and, in generally, personalization data). Updating such data can only be done by the personalization agent prior to the operational phase. Thus such data cannot be changed after the personalization of the document, as required by OT.AC\_Pers\_EAC2. Finally, FMT\_MTD.1/KEY\_READ ensures that cryptographic keys for EAC2 can not be read by users.

**OT.CA2** The security objective OT.CA2 aims at enabling verification of the authenticity of the TOE as a whole device. This objective is mainly achieved by FIA\_API.1/CA using FCS\_CKM.1/DH\_PACE. CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT\_MTD.1/SK\_PICC governs creating/loading SKPICC, whereas FMT\_MTD.1/KEY\_READ requires making this key unreadable by users. Hence, its value remains confidential. FDP\_RIP.1 requires erasing the values of SKPICC and the session keys, here for CMAC. The authentication token TPICC is calculated using FCS\_COP.1/PACE\_MAC. The SFRs FCS\_COP.1/SHA and FCS\_RND.1 represent the general required support for cryptographic operations. FMT\_MTD.1/PA requires that the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication is allowed to be modified only by the personalization agent only. Hence is to consider as trustworthy.

**OT.Sens\_Data\_EAC2** The security objective of OT.Sens\_Data\_EAC2 aims to explicitly protect sensitive (as opposed to common) user and TSF-Data. This is mainly achieved by enforcing (FDP\_UCT.1/TRM and FDP\_UIT.1/TRM) the access control SFPs FDP\_ACC.1/TRM and FDP\_ACF.1/TRM. A specific authorization level is achieved by terminal identification/authentication as required by the SFRs FIA\_UID.1/EAC2\_Terminal, FIA\_UAU.1/EAC2\_Terminal, supported by FCS\_COP.1/SIG\_VER. The TA2 protocol uses the result of the PACE authentication (FIA\_UID.1/PACE, FIA\_UAU.1/PACE, confidentiality of the PACE passwords is ensured by FMT\_MTD.1/KEY\_READ) being, in turn, supported by FCS\_CKM.1/DH\_PACE. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA\_AFL.1/Suspend\_PIN, FIA\_AFL.1/Block\_PIN, FMT\_MTD.1/Resume\_PIN, FMT\_MTD.1/Unblock\_PIN, FMT\_MTD.1/Initialize\_PIN, FMT\_MTD.1/Change\_PIN) also support to achieve this objective. FDP\_RIP.1 requires erasing the temporal values of the PIN and PUK. FIA\_UAU.4/PACE, FIA\_UAU.5/PACE, FIA\_UAU.6/PACE and FCS\_CKM.4 represent some specific properties of the used protocols. To allow for a verification of the certificate chain as required in FMT\_MTD.3, the CVCA's public key and certificate as well as the current date are written or updated by authorized identified role as required by FMT\_MTD.1/CVCA\_INI, FMT\_MTD.1/CVCA\_UPD and FMT\_MTD.1/DATE. This objective for the data exchanged is mainly achieved by FTP\_ITC.1/CA2 and FTP\_ITC.1/PACE using FCS\_COP.1/PACE\_ENC. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. FIA\_API.1/CA using FCS\_CKM.1/DH\_PACE and possessing the special properties FIA\_UAU.5/PACE, and FIA\_UAU.6/CA. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA\_UID.1/PACE, FIA\_UAU.1/PACE and FCS\_CKM.1/DH\_PACE and possessing the special properties FIA\_UAU.5/PACE, FIA\_UAU.6/PACE. CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT\_MTD.1/SK\_PICC governs creating/loading SKPICC, FMT\_MTD.1/KEY\_READ requires making this key unreadable by users. Thus its value remains confidential. FDP\_RIP.1 requires erasing the

	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>110/142</b>
---	--	---

values of SKPICC and session keys, here for KENC.FMT\_MTD.1/PA requires that only the personalization agent is allowed to modify the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication. The SFRs FCS\_COP.1/SHA and FCS\_RND.1 represent the general required support for cryptographic operations. The SFRs FMT\_SMF.1 and FMT\_SMR.1/PACE support the related functions and roles.

**OT.Data\_Authenticity** The security objective OT.Data\_Authenticity ensures the authenticity of user- and TSF-Data (after Terminal- and the Chip Authentication 2) by enabling its verification on both the terminal-side and by an active verification by the TOE itself. This objective is mainly achieved by FTP\_ITC.1/CA2 and FTP\_ITC.1/PACE using FCS\_COP.1/PACE\_MAC. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. FIA\_API.1/CA using FCS\_CKM.1/DH\_PACE and possessing the special properties FIA\_UAU.5/PACE, and FIA\_UAU.6/CA. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA\_UID.1/PACE, FIA\_UAU.1/PACE and FCS\_CKM.1/DH\_PACE and possessing the special properties FIA\_UAU.5/PACE, FIA\_UAU.6/PACE. CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT\_MTD.1/SK\_PICC governs creating/loading SKPICC, FMT\_MTD.1/KEY\_READ requires to make this key unreadable by users. Hence its value remains confidential. FDP\_RIP.1 requires to erase the values of SKPICC and session keys, here for KMAC. FMT\_MTD.1/PA requires that the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication is allowed to be modified only by the personalization agent only. Hence is to consider as trustworthy. A prerequisite for successful CA2 is an accomplished TA2 as required by FIA\_UID.1/EAC2\_Terminal, FIA\_UAU.1/EAC2\_Terminal, supported by FCS\_COP.1/SIG\_VER. The TA2 protocol uses the result of the PACE authentication (FIA\_UID.1/PACE, FIA\_UAU.1/PACE) being, in turn, supported by FCS\_CKM.1/DH\_PACE. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA\_AFL.1/Suspend\_PIN, FIA\_AFL.1/Block\_PIN, FMT\_MTD.1/Resume\_PIN, FMT\_MTD.1/Initialize\_PIN, FMT\_MTD.1/Change\_PIN, FMT\_MTD.1/Unblock\_PIN) also support achieving this objective. FDP\_RIP.1 requires to erase the temporal values of the PIN and PUK. FIA\_UAU.4/PACE, FIA\_UAU.5/PACE, FIA\_UAU.6/CA and FCS\_CKM.4 represent some specific required properties of the used protocols. To allow for a verification of the certificate chain as required in FMT\_MTD.3, the CVCA's public key and certificate, as well as the current date, are written or updated by authorized identified roles as required by FMT\_MTD.1/CVCA\_INI, FMT\_MTD.1/CVCA\_UPD and FMT\_MTD.1/DATE. The SFRs FCS\_COP.1/SHA and FCS\_RND.1 represent the general required support for cryptographic operations. The SFRs FMT\_SMF.1 and FMT\_SMR.1/PACE support the related functions and roles.

**OT.Data\_Confidentiality** The security objective OT.Data\_Confidentiality ensures that the TOE always ensures confidentiality of the user- and TSF-Data stored and, after Terminal- and Chip Authentication 2, of their exchange. This objective for the data stored is mainly achieved by FDP\_ACC.1/TRM and FDP\_ACF.1/TRM. Enforcement of the two previous in a protected manner is ensured by FDP\_UCT.1/TRM and FDP\_UIT.1/TRM. A specific authorization level is achieved by terminal identification/authentication as required by the SFRs FIA\_UID.1/EAC2\_Terminal, FIA\_UAU.1/EAC2\_Terminal, supported by FCS\_COP.1/SIG\_VER. The TA2 protocol uses the result of the PACE authentication (FIA\_UID.1/PACE, FIA\_UAU.1/PACE, confidentiality of the PACE passwords is ensured by FMT\_MTD.1/KEY\_READ) being, in turn, supported by FCS\_CKM.1/DH\_PACE. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA\_AFL.1/Suspend\_PIN, FIA\_AFL.1/Block\_PIN, FMT\_MTD.1/Resume\_PIN, FMT\_MTD.1/Unblock\_PIN, FMT\_MTD.1/Change\_PIN, FMT\_MTD.1/Initialize\_PIN) also



support to achieve this objective. FDP\_RIP.1 requires erasing the temporal values of the PIN and PUK. FIA\_UAU.4/PACE, FIA\_UAU.5/PACE, FIA\_UAU.6/PACE and FCS\_CKM.4 represent some specific properties of the used protocols. To allow for a verification of the certificate chain as required in FMT\_MTD.3, the CVCA's public key and certificate as well as the current date are written or updated by authorized identified role as required by FMT\_MTD.1/CVCA\_INI, FMT\_MTD.1/CVCA\_UPD and FMT\_MTD.1/DATE. This objective for the data exchanged is mainly achieved by FTP\_ITC.1/CA2 and FTP\_ITC.1/PACE using FCS\_COP.1/PACE\_ENC. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. FIA\_API.1/CA using FCS\_CKM.1/DH\_PACE and possessing the special properties FIA\_UAU.5/PACE, and FIA\_UAU.6/CA. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA\_UID.1/PACE, FIA\_UAU.1/PACE and FCS\_CKM.1/DH\_PACE and possessing the special properties FIA\_UAU.5/PACE, FIA\_UAU.6/PACE. CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT\_MTD.1/SK\_PICC governs creating/loading SKPICC, FMT\_MTD.1/KEY\_READ requires making this key unreadable by users. Thus its value remains confidential. FDP\_RIP.1 requires erasing the values of SKPICC and session keys, here for KENC. FMT\_MTD.1/PA requires that only the personalization agent is allowed to modify the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication. The SFRs FCS\_COP.1/SHA and FCS\_RND.1 represent the general required support for cryptographic operations. The SFRs FMT\_SMF.1 and FMT\_SMR.1/PACE support the related functions and roles.

**OT.Data\_Integrity** The security objective OT.Data\_Integrity ensures that the TOE always ensures integrity of stored user- and TSF-Data and, after Terminal- and Chip Authentication 2, of these data exchanged (physical manipulation and unauthorized modifying). Physical manipulation is addressed by FPT\_PHP.3. Unauthorized modifying of the stored data is addressed by FDP\_ACC.1/TRM and FDP\_ACF.1/TRM. Enforcement of the two previous in a protected manner is ensured by FDP\_UCT.1/TRM and FDP\_UIT.1/TRM. A specific authorization level is achieved by terminal identification/ authentication as required by the SFRs FIA\_UID.1/EAC2\_Terminal, FIA\_UAU.1/EAC2\_Terminal, supported by FCS\_COP.1/SIG\_VER. The TA2 protocol uses the result of PACE authentication (FIA\_UID.1/PACE, FIA\_UAU.1/PACE) being, in turn, supported by FCS\_CKM.1/DH\_PACE. Since PACE can use the PIN as the shared secret, using and management of PIN (FIA\_AFL.1/Suspend\_PIN, FIA\_AFL.1/Block\_PIN, FMT\_MTD.1/Resume\_PIN, FMT\_MTD.1/Change\_PIN, FMT\_MTD.1/Unblock\_PIN, FMT\_MTD.1/Initialize\_PIN) also support achievement of this objective. FDP\_RIP.1 requires erasing the temporal values of PIN, PUK. FIA\_UAU.4/PACE, FIA\_UAU.5/PACE and FCS\_CKM.4 represent some required specific properties of the used protocols. To allow for a verification of the certificate chain as required in FMT\_MTD.3, the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as required by FMT\_MTD.1/CVCA\_INI, FMT\_MTD.1/CVCA\_UPD and FMT\_MTD.1/DATE. Unauthorized modifying of the exchanged data is addressed by FTP\_ITC.1/CA2 and FTP\_ITC.1/PACE using FCS\_COP.1/PACE\_MAC. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. FIA\_API.1/CA using FCS\_CKM.1/DH\_PACE possessing the special properties FIA\_UAU.5/PACE and FIA\_UAU.6/CA. As a prerequisite of this trusted channel a trusted channel established with the PACE protocol using FIA\_UID.1/PACE, FIA\_UAU.1/PACE and FCS\_CKM.1/DH\_PACE and possessing the special properties FIA\_UAU.5/PACE, FIA\_UAU.6/PACE. CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT\_MTD.1/SK\_PICC governs creating/loading SKPICC, and FMT\_MTD.1/KEY\_READ requires SKPICC to be unreadable by users; thus its value remains confidential. FDP\_RIP.1 requires erasing the values of SKPICC and session keys (here: for

KMAC).FMT\_MTD.1/PA requires that the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication is allowed to be modified only by the personalization agent. Hence, is to considered as trustworthy.The SFRs FCS\_COP.1/SHA and FCS\_RND.1 represent general support required for cryptographic operations.The SFRs FMT\_SMF.1 and FMT\_SMR.1/PACE support related functions and roles.

**OT.Identification** The security objective OT.Identification addresses the storage of Initialisation and Pre-Personalisation Data in its non-volatile memory, whereby they also include the IC Identification Data uniquely identifying the TOE's chip. The SFR FMT\_MTD.1/INI\_ENA allows only the Manufacturer to write Initialisation and Pre-personalisation Data (including the Personalisation Agent key). The SFR FMT\_MTD.1/INI\_DIS requires the Personalisation Agent to disable access to Initialisation and Pre-personalisation Data in the life cycle phase 'operational use'.The SFRs FMT\_SMF.1 and FMT\_SMR.1/PACE support the functions and roles related.

**OT.Prot\_Abuse-Func** The security objective OT.Prot\_Abuse\_Func aims preventing TOE's functions being not intended to be used in the operational phase from manipulating and disclosing the User- and TSF-data.This objective is achieved by FMT\_LIM.1 and FMT\_LIM.2 preventing misuse of test and other functionality of the TOE having not to be used in the TOE's operational life cycle phase.

**OT.Prot\_Inf\_Leak** The security objective OT.Prot\_Inf\_Leak aims protection against disclosure of confidential User- or/and TSF-data stored on / processed by the TOE. This objective is achieved

- o by FPT\_EMS.1 for measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
- o by FPT\_FLS.1 and FPT\_TST.1 for forcing a malfunction of the TOE, and
- o by FPT\_PHP.3 for a physical manipulation of the TOE.

**OT.Prot\_Malfunction** The security objective OT.Prot\_Malfunction aims ensuring a correct operation of the TOE by preventing its operation outside the normal operating conditions.This objective is covered by FPT\_TST.1 requiring self tests to demonstrate the correct operation of the TOE and tests of authorised users to verify the integrity of the TSF-data and the embedded software (TSF code) as well as by FPT\_FLS.1 requiring entering a secure state of the TOE in case of detected failure or operating conditions possibly causing a malfunction.

**OT.Prot\_Phys-Tamper** The security objective OT.Prot\_Phys-Tamper aims protection of the confidentiality and integrity of the User- and TSF-data as well as embedded software stored in the TOE.This objective is completely covered by FPT\_PHP.3 in an obvious way.

**OT.Tracing** The security objective OT.Tracing ensures that the TOE prevents gathering TOE tracing data by means of unambiguously identifying the electronic document remotely through establishing or listening to communication via the contactless/contact-based interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ, PIN, PUK).This objective is achieved as follows: 1.While establishing PACE communication with CAN, MRZ or PUK (non-blocking authentication / authorization data)



by FIA\_AFL.1/PACE while establishing PACE communication using the PIN (blocking authentication data) by FIA\_AFL.1/Block\_PIN 3.for listening to PACE communication and for establishing CA2 communication (which is of importance for the current PP, if Chip Security Object and PKPICC are card-individual) by FTP\_ITC.1/PACE, 4.and for listening to CA2 communication (readable and writable user data: document details data, biographic data, biometric reference data) by FTP\_ITC.1/CA2.

### 9.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
<a href="#">OT.Tamper Resistance</a>	<a href="#">FPT_PHP.3</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Tamper ID</a>	<a href="#">FPT_PHP.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.EMSEC Design</a>	<a href="#">FPT_EMS.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.DTBS Integrity TOE</a>	<a href="#">FDP_SDI.2/DTBS</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Sigy SigF</a>	<a href="#">FDP_ACF.1/Signature Creation</a> , <a href="#">FDP_ACC.1/Signature Creation</a> , <a href="#">FDP_RIP.1</a> , <a href="#">FDP_SDI.2/DTBS</a> , <a href="#">FIA_AFL.1</a> , <a href="#">FIA_UAU.1</a> , <a href="#">FIA_UID.1</a> , <a href="#">FMT_MOF.1</a> , <a href="#">FMT_MSA.1/Signatory</a> , <a href="#">FMT_MSA.2</a> , <a href="#">FMT_MSA.3</a> , <a href="#">FMT_MSA.4</a> , <a href="#">FMT_MTD.1/Admin</a> , <a href="#">FMT_MTD.1/Signatory</a> , <a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Sig Secure</a>	<a href="#">FDP_SDI.2/Persistent</a> , <a href="#">FPT_TST.1</a> , <a href="#">FCS_COP.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.SCD Secrecy</a>	<a href="#">FCS_CKM.1</a> , <a href="#">FCS_CKM.4</a> , <a href="#">FDP_RIP.1</a> , <a href="#">FDP_SDI.2/Persistent</a> , <a href="#">FPT_FLS.1</a> , <a href="#">FPT_PHP.3</a> , <a href="#">FPT_TST.1</a> , <a href="#">FPT_EMS.1</a> , <a href="#">FDP_UCT.1/SCD</a> , <a href="#">FTP_ITC.1/SCD</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Lifecycle Security</a>	<a href="#">FCS_CKM.1</a> , <a href="#">FCS_CKM.4</a> , <a href="#">FDP_ACC.1/SCD/SVD Generation</a> , <a href="#">FDP_ACF.1/SCD/SVD Generation</a> , <a href="#">FDP_ACC.1/SVD Transfer</a> , <a href="#">FDP_ACF.1/Signature Creation</a> , <a href="#">FDP_ACC.1/Signature Creation</a> , <a href="#">FDP_ACF.1/SVD Transfer</a> , <a href="#">FMT_MOF.1</a> , <a href="#">FMT_MSA.1/Admin</a> , <a href="#">FMT_MSA.1/Signatory</a> , <a href="#">FMT_MTD.1/Unblock PIN</a> , <a href="#">FMT_MSA.2</a> , <a href="#">FMT_MSA.3</a> , <a href="#">FMT_MSA.4</a> , <a href="#">FMT_MTD.1/Admin</a> , <a href="#">FMT_MTD.1/Signatory</a> , <a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FPT_TST.1</a> , <a href="#">FCS_COP.1</a> , <a href="#">FDP_ACC.1/SCD Import</a> , <a href="#">FDP_ACF.1/SCD Import</a> , <a href="#">FDP_ITC.1/SCD</a> , <a href="#">FDP_UCT.1/SCD</a> , <a href="#">FTP_ITC.1/SCD</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.SCD SVD Corresp</a>	<a href="#">FCS_CKM.1</a> , <a href="#">FDP_SDI.2/Persistent</a> , <a href="#">FMT_MSA.4</a> , <a href="#">FMT_SMF.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.SCD Unique</a>	<a href="#">FCS_CKM.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.SCD/SVD Gen</a>	<a href="#">FDP_ACC.1/SCD/SVD Generation</a> , <a href="#">FDP_ACF.1/SCD/SVD Generation</a> , <a href="#">FIA_UAU.1</a> ,	<a href="#">Section 9.3.1</a>

	<a href="#">FIA UID.1</a> , <a href="#">FMT MSA.1/Admin</a> , <a href="#">FMT MSA.2</a> , <a href="#">FMT MSA.3</a> , <a href="#">FMT MSA.4</a>	
<a href="#">OT.SCD Auth Imp</a>	<a href="#">FIA UID.1</a> , <a href="#">FIA UAU.1</a> , <a href="#">FDP ACC.1/SCD Import</a> , <a href="#">FDP ACF.1/SCD Import</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.TOE SSCD Auth</a>	<a href="#">FIA UAU.1</a> , <a href="#">FIA API.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.TOE TC SVD Exp</a>	<a href="#">FDP ACF.1/SVD Transfer</a> , <a href="#">FDP ACC.1/SVD Transfer</a> , <a href="#">FDP DAU.2/SVD</a> , <a href="#">FTP ITC.1/SVD</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.TOE TC VAD Imp</a>	<a href="#">FTP ITC.1/VAD</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.TOE TC DTBS Imp</a>	<a href="#">FDP UIT.1/DTBS</a> , <a href="#">FTP ITC.1/DTBS</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.AC Pers EAC2</a>	<a href="#">FIA AFL.1/Suspend PIN</a> , <a href="#">FIA AFL.1/Block PIN</a> , <a href="#">FIA UAU.1/EAC2 Terminal</a> , <a href="#">FIA UID.1/EAC2 Terminal</a> , <a href="#">FDP ACF.1/TRM</a> , <a href="#">FDP RIP.1</a> , <a href="#">FDP ACC.1/TRM</a> , <a href="#">FMT SMF.1</a> , <a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT MTD.1/PA</a> , <a href="#">FMT MTD.1/KEY READ</a> , <a href="#">FMT MTD.1/Initialize PIN</a> , <a href="#">FMT MTD.1/Resume PIN</a> , <a href="#">FMT MTD.1/Change PIN</a> , <a href="#">FMT MTD.1/Unblock PIN</a> , <a href="#">FMT MTD.1/INI ENA</a> , <a href="#">FMT MTD.1/INI DIS</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.CA2</a>	<a href="#">FCS CKM.1/DH PACE</a> , <a href="#">FCS COP.1/SHA</a> , <a href="#">FCS COP.1/PACE MAC</a> , <a href="#">FCS RND.1</a> , <a href="#">FIA API.1/CA</a> , <a href="#">FDP RIP.1</a> , <a href="#">FMT MTD.1/PA</a> , <a href="#">FMT MTD.1/SK PICC</a> , <a href="#">FMT MTD.1/KEY READ</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Sens Data EAC2</a>	<a href="#">FTP ITC.1/CA2</a> , <a href="#">FCS RND.1</a> , <a href="#">FCS CKM.1/DH PACE</a> , <a href="#">FCS COP.1/SHA</a> , <a href="#">FCS COP.1/SIG VER</a> , <a href="#">FCS COP.1/PACE ENC</a> , <a href="#">FIA UAU.1/PACE</a> , <a href="#">FIA UAU.5/PACE</a> , <a href="#">FIA AFL.1/Suspend PIN</a> , <a href="#">FIA AFL.1/Block PIN</a> , <a href="#">FIA UAU.1/EAC2 Terminal</a> , <a href="#">FIA API.1/CA</a> , <a href="#">FIA UAU.6/CA</a> , <a href="#">FIA UID.1/PACE</a> , <a href="#">FIA UID.1/EAC2 Terminal</a> , <a href="#">FIA UAU.4/PACE</a> , <a href="#">FIA UAU.6/PACE</a> , <a href="#">FDP ACF.1/TRM</a> , <a href="#">FDP ACC.1/TRM</a> , <a href="#">FDP UCT.1/TRM</a> , <a href="#">FDP UIT.1/TRM</a> , <a href="#">FTP ITC.1/PACE</a> , <a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT MTD.1/CVCA INI</a> , <a href="#">FMT MTD.1/CVCA UPD</a> , <a href="#">FMT MTD.1/DATE</a> , <a href="#">FMT MTD.1/PA</a> , <a href="#">FMT MTD.1/SK PICC</a> , <a href="#">FMT MTD.1/KEY READ</a> , <a href="#">FMT MTD.1/Initialize PIN</a> , <a href="#">FMT MTD.1/Resume PIN</a> , <a href="#">FMT MTD.1/Change PIN</a> , <a href="#">FMT MTD.1/Unblock PIN</a> , <a href="#">FMT MTD.3</a> , <a href="#">FMT SMF.1</a> , <a href="#">FCS CKM.4</a> , <a href="#">FDP RIP.1</a>	<a href="#">Section 9.3.1</a>

<a href="#">OT.Data Authenticity</a>	<a href="#">FTP ITC.1/CA2</a> , <a href="#">FCS RND.1</a> , <a href="#">FCS CKM.1/DH PACE</a> , <a href="#">FCS COP.1/SHA</a> , <a href="#">FCS COP.1/SIG VER</a> , <a href="#">FCS COP.1/PACE MAC</a> , <a href="#">FIA UAU.1/PACE</a> , <a href="#">FIA UAU.5/PACE</a> , <a href="#">FIA AFL.1/Suspend PIN</a> , <a href="#">FIA AFL.1/Block PIN</a> , <a href="#">FIA UAU.1/EAC2 Terminal</a> , <a href="#">FIA API.1/CA</a> , <a href="#">FIA UAU.6/CA</a> , <a href="#">FIA UID.1/PACE</a> , <a href="#">FIA UID.1/EAC2 Terminal</a> , <a href="#">FIA UAU.4/PACE</a> , <a href="#">FIA UAU.6/PACE</a> , <a href="#">FTP ITC.1/PACE</a> , <a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT MTD.1/CVCA INI</a> , <a href="#">FMT MTD.1/CVCA UPD</a> , <a href="#">FMT MTD.1/DATE</a> , <a href="#">FMT MTD.1/PA</a> , <a href="#">FMT MTD.1/SK PICC</a> , <a href="#">FMT MTD.1/KEY READ</a> , <a href="#">FMT MTD.1/Initialize PIN</a> , <a href="#">FMT MTD.1/Resume PIN</a> , <a href="#">FMT MTD.1/Change PIN</a> , <a href="#">FMT MTD.1/Unblock PIN</a> , <a href="#">FMT MTD.3</a> , <a href="#">FMT SMF.1</a> , <a href="#">FCS CKM.4</a> , <a href="#">FDP RIP.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Data Confidentiality</a>	<a href="#">FTP ITC.1/CA2</a> , <a href="#">FCS RND.1</a> , <a href="#">FCS CKM.1/DH PACE</a> , <a href="#">FCS COP.1/SHA</a> , <a href="#">FCS COP.1/SIG VER</a> , <a href="#">FCS COP.1/PACE ENC</a> , <a href="#">FIA UAU.1/PACE</a> , <a href="#">FIA UAU.5/PACE</a> , <a href="#">FIA AFL.1/Suspend PIN</a> , <a href="#">FIA AFL.1/Block PIN</a> , <a href="#">FIA UAU.1/EAC2 Terminal</a> , <a href="#">FIA API.1/CA</a> , <a href="#">FIA UAU.6/CA</a> , <a href="#">FIA UID.1/PACE</a> , <a href="#">FIA UID.1/EAC2 Terminal</a> , <a href="#">FIA UAU.4/PACE</a> , <a href="#">FIA UAU.6/PACE</a> , <a href="#">FDP ACF.1/TRM</a> , <a href="#">FDP ACC.1/TRM</a> , <a href="#">FDP UCT.1/TRM</a> , <a href="#">FDP UIT.1/TRM</a> , <a href="#">FTP ITC.1/PACE</a> , <a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT MTD.1/CVCA INI</a> , <a href="#">FMT MTD.1/CVCA UPD</a> , <a href="#">FMT MTD.1/DATE</a> , <a href="#">FMT MTD.1/PA</a> , <a href="#">FMT MTD.1/SK PICC</a> , <a href="#">FMT MTD.1/KEY READ</a> , <a href="#">FMT MTD.1/Initialize PIN</a> , <a href="#">FMT MTD.1/Resume PIN</a> , <a href="#">FMT MTD.1/Change PIN</a> , <a href="#">FMT MTD.1/Unblock PIN</a> , <a href="#">FMT MTD.3</a> , <a href="#">FMT SMF.1</a> , <a href="#">FCS CKM.4</a> , <a href="#">FDP RIP.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Data Integrity</a>	<a href="#">FTP ITC.1/CA2</a> , <a href="#">FCS RND.1</a> , <a href="#">FCS CKM.1/DH PACE</a> , <a href="#">FCS COP.1/SHA</a> , <a href="#">FCS COP.1/SIG VER</a> , <a href="#">FCS COP.1/PACE MAC</a> , <a href="#">FIA UAU.1/PACE</a> , <a href="#">FIA UAU.5/PACE</a> , <a href="#">FIA AFL.1/Suspend PIN</a> , <a href="#">FIA AFL.1/Block PIN</a> , <a href="#">FIA UAU.1/EAC2 Terminal</a> , <a href="#">FIA API.1/CA</a> , <a href="#">FIA UAU.6/CA</a> , <a href="#">FIA UID.1/PACE</a> , <a href="#">FIA UID.1/EAC2 Terminal</a> , <a href="#">FIA UAU.4/PACE</a> , <a href="#">FIA UAU.6/PACE</a> , <a href="#">FDP ACF.1/TRM</a> , <a href="#">FDP ACC.1/TRM</a> , <a href="#">FDP UCT.1/TRM</a> , <a href="#">FDP UIT.1/TRM</a> , <a href="#">FTP ITC.1/PACE</a> , <a href="#">FMT SMR.1/PACE</a> , <a href="#">FMT MTD.1/CVCA INI</a> ,	<a href="#">Section 9.3.1</a>

	<a href="#">FMT_MTD.1/CVCA_UPD</a> , <a href="#">FMT_MTD.1/DATE</a> , <a href="#">FMT_MTD.1/PA</a> , <a href="#">FMT_MTD.1/SK_PICC</a> , <a href="#">FMT_MTD.1/KEY_READ</a> , <a href="#">FMT_MTD.1/Initialize_PIN</a> , <a href="#">FMT_MTD.1/Resume_PIN</a> , <a href="#">FMT_MTD.1/Change_PIN</a> , <a href="#">FMT_MTD.1/Unblock_PIN</a> , <a href="#">FMT_MTD.3</a> , <a href="#">FPT_PHP.3</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FCS_CKM.4</a> , <a href="#">FDP_RIP.1</a>	
<a href="#">OT.Identification</a>	<a href="#">FMT_SMF.1</a> , <a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_MTD.1/INI_ENA</a> , <a href="#">FMT_MTD.1/INI_DIS</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Prot_Abuse-Func</a>	<a href="#">FMT_LIM.1</a> , <a href="#">FMT_LIM.2</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Prot_Inf_Leak</a>	<a href="#">FPT_FLS.1</a> , <a href="#">FPT_TST.1</a> , <a href="#">FPT_PHP.3</a> , <a href="#">FPT_EMS.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Prot_Malfunction</a>	<a href="#">FPT_FLS.1</a> , <a href="#">FPT_TST.1</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Prot_Phys-Tamper</a>	<a href="#">FPT_PHP.3</a>	<a href="#">Section 9.3.1</a>
<a href="#">OT.Tracing</a>	<a href="#">FIA_AFL.1/Block_PIN</a> , <a href="#">FIA_AFL.1/PACE</a> , <a href="#">FTP_ITC.1/CA2</a> , <a href="#">FTP_ITC.1/PACE</a>	<a href="#">Section 9.3.1</a>

**Table 10 Security Objectives and SFRs - Coverage**

Security Functional Requirements	Security Objectives	Rationale
<a href="#">FPT_EMS.1</a>	<a href="#">OT.EMSEC_Design</a> , <a href="#">OT.SCD_Secrecy</a> , <a href="#">OT.Prot_Inf_Leak</a>	
<a href="#">FPT_FLS.1</a>	<a href="#">OT.SCD_Secrecy</a> , <a href="#">OT.Prot_Inf_Leak</a> , <a href="#">OT.Prot_Malfunction</a>	
<a href="#">FPT_PHP.1</a>	<a href="#">OT.Tamper_ID</a>	
<a href="#">FPT_PHP.3</a>	<a href="#">OT.Tamper_Resistance</a> , <a href="#">OT.SCD_Secrecy</a> , <a href="#">OT.Data_Integrity</a> , <a href="#">OT.Prot_Inf_Leak</a> , <a href="#">OT.Prot_Phys-Tamper</a>	
<a href="#">FPT_TST.1</a>	<a href="#">OT.Sig_Secure</a> , <a href="#">OT.SCD_Secrecy</a> , <a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.Prot_Inf_Leak</a> , <a href="#">OT.Prot_Malfunction</a>	
<a href="#">FMT_SMR.1</a>	<a href="#">OT.Sigy_SigF</a> , <a href="#">OT.Lifecycle_Security</a>	
<a href="#">FMT_SMF.1</a>	<a href="#">OT.Sigy_SigF</a> , <a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.SCD_SVD_Corresp</a> , <a href="#">OT.AC_Pers_EAC2</a> , <a href="#">OT.Sens_Data_EAC2</a> , <a href="#">OT.Data_Authenticity</a> , <a href="#">OT.Data_Confidentiality</a> , <a href="#">OT.Data_Integrity</a> , <a href="#">OT.Identification</a>	
<a href="#">FMT_MOF.1</a>	<a href="#">OT.Sigy_SigF</a> , <a href="#">OT.Lifecycle_Security</a>	
<a href="#">FMT_MSA.1/Admin</a>	<a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.SCD/SVD_Gen</a>	
<a href="#">FMT_MSA.1/Signatory</a>	<a href="#">OT.Sigy_SigF</a> , <a href="#">OT.Lifecycle_Security</a>	
<a href="#">FMT_MSA.2</a>	<a href="#">OT.Sigy_SigF</a> , <a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.SCD/SVD_Gen</a>	

<a href="#">FMT_MSA.3</a>	<a href="#">OT.Sigy_SigF</a> , <a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.SCD/SVD_Gen</a>	
<a href="#">FMT_MSA.4</a>	<a href="#">OT.Sigy_SigF</a> , <a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.SCD_SVD_Corresp</a> , <a href="#">OT.SCD/SVD_Gen</a>	
<a href="#">FMT_MTD.1/Admin</a>	<a href="#">OT.Sigy_SigF</a> , <a href="#">OT.Lifecycle_Security</a>	
<a href="#">FMT_MTD.1/Signatory</a>	<a href="#">OT.Sigy_SigF</a> , <a href="#">OT.Lifecycle_Security</a>	
<a href="#">FIA_UID.1</a>	<a href="#">OT.Sigy_SigF</a> , <a href="#">OT.SCD/SVD_Gen</a> , <a href="#">OT.SCD_Auth_Imp</a>	
<a href="#">FIA_AFL.1</a>	<a href="#">OT.Sigy_SigF</a>	
<a href="#">FIA_UAU.1</a>	<a href="#">OT.Sigy_SigF</a> , <a href="#">OT.SCD/SVD_Gen</a> , <a href="#">OT.SCD_Auth_Imp</a> , <a href="#">OT.TOE_SSCD_Auth</a>	
<a href="#">FDP_SDI.2/DTBS</a>	<a href="#">OT.DTBS_Integrity_TOE</a> , <a href="#">OT.Sigy_SigF</a>	
<a href="#">FDP_SDI.2/Persistent</a>	<a href="#">OT.Sig_Secure</a> , <a href="#">OT.SCD_Secrecy</a> , <a href="#">OT.SCD_SVD_Corresp</a>	
<a href="#">FDP_RIP.1</a>	<a href="#">OT.Sigy_SigF</a> , <a href="#">OT.SCD_Secrecy</a> , <a href="#">OT.AC_Pers_EAC2</a> , <a href="#">OT.CA2</a> , <a href="#">OT.Sens_Data_EAC2</a> , <a href="#">OT.Data_Authenticity</a> , <a href="#">OT.Data_Confidentiality</a> , <a href="#">OT.Data_Integrity</a>	
<a href="#">FDP_ACC.1/Signature_Creation</a>	<a href="#">OT.Sigy_SigF</a> , <a href="#">OT.Lifecycle_Security</a>	
<a href="#">FDP_ACF.1/Signature_Creation</a>	<a href="#">OT.Sigy_SigF</a> , <a href="#">OT.Lifecycle_Security</a>	
<a href="#">FCS_COP.1</a>	<a href="#">OT.Sig_Secure</a> , <a href="#">OT.Lifecycle_Security</a>	
<a href="#">FCS_CKM.4</a>	<a href="#">OT.SCD_Secrecy</a> , <a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.Sens_Data_EAC2</a> , <a href="#">OT.Data_Authenticity</a> , <a href="#">OT.Data_Confidentiality</a> , <a href="#">OT.Data_Integrity</a>	
<a href="#">FCS_CKM.1</a>	<a href="#">OT.SCD_Secrecy</a> , <a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.SCD_SVD_Corresp</a> , <a href="#">OT.SCD_Unique</a>	
<a href="#">FDP_ACC.1/SVD_Transfer</a>	<a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.TOE_TC_SVD_Exp</a>	
<a href="#">FDP_ACF.1/SVD_Transfer</a>	<a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.TOE_TC_SVD_Exp</a>	
<a href="#">FDP_ACC.1/SCD/SVD_Generation</a>	<a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.SCD/SVD_Gen</a>	
<a href="#">FDP_ACF.1/SCD/SVD_Generation</a>	<a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.SCD/SVD_Gen</a>	
<a href="#">FTP_ITC.1/SCD</a>	<a href="#">OT.SCD_Secrecy</a> , <a href="#">OT.Lifecycle_Security</a>	
<a href="#">FDP_UCT.1/SCD</a>	<a href="#">OT.SCD_Secrecy</a> , <a href="#">OT.Lifecycle_Security</a>	
<a href="#">FDP_ITC.1/SCD</a>	<a href="#">OT.Lifecycle_Security</a>	
<a href="#">FDP_ACC.1/SCD_Import</a>	<a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.SCD_Auth_Imp</a>	
<a href="#">FDP_ACF.1/SCD_Import</a>	<a href="#">OT.Lifecycle_Security</a> , <a href="#">OT.SCD_Auth_Imp</a>	
<a href="#">FTP_ITC.1/SVD</a>	<a href="#">OT.TOE_TC_SVD_Exp</a>	

<a href="#">FDP_DAU.2/SVD</a>	<a href="#">OT.TOE TC SVD Exp</a>	
<a href="#">FIA_API.1</a>	<a href="#">OT.TOE SSCD Auth</a>	
<a href="#">FDP_UIT.1/DTBS</a>	<a href="#">OT.TOE TC DTBS Imp</a>	
<a href="#">FTP_ITC.1/VAD</a>	<a href="#">OT.TOE TC VAD Imp</a>	
<a href="#">FTP_ITC.1/DTBS</a>	<a href="#">OT.TOE TC DTBS Imp</a>	
<a href="#">FCS_RND.1</a>	<a href="#">OT.CA2, OT.Sens Data EAC2,</a> <a href="#">OT.Data Authenticity,</a> <a href="#">OT.Data Confidentiality, OT.Data Integrity</a>	
<a href="#">FCS_CKM.1/DH_PACE</a>	<a href="#">OT.CA2, OT.Sens Data EAC2,</a> <a href="#">OT.Data Authenticity,</a> <a href="#">OT.Data Confidentiality, OT.Data Integrity</a>	
<a href="#">FCS_COP.1/SHA</a>	<a href="#">OT.CA2, OT.Sens Data EAC2,</a> <a href="#">OT.Data Authenticity,</a> <a href="#">OT.Data Confidentiality, OT.Data Integrity</a>	
<a href="#">FCS_COP.1/SIG_VER</a>	<a href="#">OT.Sens Data EAC2, OT.Data Authenticity,</a> <a href="#">OT.Data Confidentiality, OT.Data Integrity</a>	
<a href="#">FCS_COP.1/PACE_ENC</a>	<a href="#">OT.Sens Data EAC2,</a> <a href="#">OT.Data Confidentiality</a>	
<a href="#">FCS_COP.1/PACE_MAC</a>	<a href="#">OT.CA2, OT.Data Authenticity,</a> <a href="#">OT.Data Integrity</a>	
<a href="#">FIA_UAU.1/PACE</a>	<a href="#">OT.Sens Data EAC2, OT.Data Authenticity,</a> <a href="#">OT.Data Confidentiality, OT.Data Integrity</a>	
<a href="#">FIA_UAU.5/PACE</a>	<a href="#">OT.Sens Data EAC2, OT.Data Authenticity,</a> <a href="#">OT.Data Confidentiality, OT.Data Integrity</a>	
<a href="#">FIA_AFL.1/Suspend_PIN</a>	<a href="#">OT.AC Pers EAC2, OT.Sens Data EAC2,</a> <a href="#">OT.Data Authenticity,</a> <a href="#">OT.Data Confidentiality, OT.Data Integrity</a>	
<a href="#">FIA_AFL.1/Block_PIN</a>	<a href="#">OT.AC Pers EAC2, OT.Sens Data EAC2,</a> <a href="#">OT.Data Authenticity,</a> <a href="#">OT.Data Confidentiality, OT.Data Integrity,</a> <a href="#">OT.Tracing</a>	
<a href="#">FIA_AFL.1/PACE</a>	<a href="#">OT.Tracing</a>	
<a href="#">FIA_UAU.1/EAC2_Terminal</a>	<a href="#">OT.AC Pers EAC2, OT.Sens Data EAC2,</a> <a href="#">OT.Data Authenticity,</a> <a href="#">OT.Data Confidentiality, OT.Data Integrity</a>	
<a href="#">FIA_API.1/CA</a>	<a href="#">OT.CA2, OT.Sens Data EAC2,</a> <a href="#">OT.Data Authenticity,</a> <a href="#">OT.Data Confidentiality, OT.Data Integrity</a>	
<a href="#">FIA_UAU.6/CA</a>	<a href="#">OT.Sens Data EAC2, OT.Data Authenticity,</a> <a href="#">OT.Data Confidentiality, OT.Data Integrity</a>	

<a href="#">FIA_UID.1/PACE</a>	<a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FIA_UID.1/EAC2 Terminal</a>	<a href="#">OT.AC Pers EAC2</a> , <a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FIA_UAU.4/PACE</a>	<a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FIA_UAU.6/PACE</a>	<a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FDP_ACF.1/TRM</a>	<a href="#">OT.AC Pers EAC2</a> , <a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FDP_ACC.1/TRM</a>	<a href="#">OT.AC Pers EAC2</a> , <a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FDP_UCT.1/TRM</a>	<a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FDP_UIT.1/TRM</a>	<a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FTP_ITC.1/PACE</a>	<a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Tracing</a>	
<a href="#">FMT_SMR.1/PACE</a>	<a href="#">OT.AC Pers EAC2</a> , <a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Identification</a>	
<a href="#">FMT_MTD.1/CVCA_INI</a>	<a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FMT_MTD.1/CVCA_UPD</a>	<a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FMT_MTD.1/DATE</a>	<a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FMT_MTD.1/PA</a>	<a href="#">OT.AC Pers EAC2</a> , <a href="#">OT.CA2</a> , <a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FMT_MTD.1/SK_PICC</a>	<a href="#">OT.CA2</a> , <a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FMT_MTD.1/KEY_READ</a>	<a href="#">OT.AC Pers EAC2</a> , <a href="#">OT.CA2</a> , <a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FMT_MTD.1/Initialize PIN</a>	<a href="#">OT.AC Pers EAC2</a> , <a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	

<a href="#">FMT_MTD.1/Resume PIN</a>	<a href="#">OT.AC Pers EAC2</a> , <a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FMT_MTD.1/Change PIN</a>	<a href="#">OT.AC Pers EAC2</a> , <a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FMT_MTD.1/Unblock PIN</a>	<a href="#">OT.Lifecycle Security</a> , <a href="#">OT.AC Pers EAC2</a> , <a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FMT_MTD.3</a>	<a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a>	
<a href="#">FMT_MTD.1/INI_ENA</a>	<a href="#">OT.AC Pers EAC2</a> , <a href="#">OT.Identification</a>	
<a href="#">FMT_MTD.1/INI_DIS</a>	<a href="#">OT.AC Pers EAC2</a> , <a href="#">OT.Identification</a>	
<a href="#">FTP_ITC.1/CA2</a>	<a href="#">OT.Sens Data EAC2</a> , <a href="#">OT.Data Authenticity</a> , <a href="#">OT.Data Confidentiality</a> , <a href="#">OT.Data Integrity</a> , <a href="#">OT.Tracing</a>	
<a href="#">FMT_LIM.1</a>	<a href="#">OT.Prot Abuse-Func</a>	
<a href="#">FMT_LIM.2</a>	<a href="#">OT.Prot Abuse-Func</a>	

**Table 11 SFRs and Security Objectives**

### 9.3.3 Dependencies

#### 9.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
<a href="#">FCS_RND.1</a>	No Dependencies	
<a href="#">FCS_CKM.1/DH_PACE</a>	( <a href="#">FCS_CKM.2</a> or <a href="#">FCS_COP.1</a> ) and ( <a href="#">FCS_CKM.4</a> )	<a href="#">FCS_COP.1</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FCS_COP.1/SHA</a>	( <a href="#">FCS_CKM.1</a> or <a href="#">FDP_ITC.1</a> or <a href="#">FDP_ITC.2</a> ) and ( <a href="#">FCS_CKM.4</a> )	<a href="#">FCS_CKM.4</a> , <a href="#">FCS_CKM.1</a>
<a href="#">FCS_COP.1/SIG_VER</a>	( <a href="#">FCS_CKM.1</a> or <a href="#">FDP_ITC.1</a> or <a href="#">FDP_ITC.2</a> ) and ( <a href="#">FCS_CKM.4</a> )	<a href="#">FCS_CKM.4</a> , <a href="#">FCS_CKM.1</a>
<a href="#">FCS_COP.1/PACE_ENC</a>	( <a href="#">FCS_CKM.1</a> or <a href="#">FDP_ITC.1</a> or <a href="#">FDP_ITC.2</a> ) and ( <a href="#">FCS_CKM.4</a> )	<a href="#">FCS_CKM.1/DH_PACE</a> , <a href="#">FCS_CKM.4</a>



<a href="#">FCS_COP.1/PACE_MAC</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.1/DH_PACE</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FIA_UAU.1/PACE</a>	(FIA_UID.1)	<a href="#">FIA_UID.1/PACE</a>
<a href="#">FIA_UAU.5/PACE</a>	No Dependencies	
<a href="#">FIA_AFL.1/Suspend_PIN</a>	(FIA_UAU.1)	<a href="#">FIA_UAU.1/PACE</a>
<a href="#">FIA_AFL.1/Block_PIN</a>	(FIA_UAU.1)	<a href="#">FIA_UAU.1/PACE</a>
<a href="#">FIA_AFL.1/PACE</a>	(FIA_UAU.1)	<a href="#">FIA_UAU.1/PACE</a>
<a href="#">FIA_UAU.1/EAC2_Terminal</a>	(FIA_UID.1)	<a href="#">FIA_UID.1/EAC2_Terminal</a>
<a href="#">FIA_API.1/CA</a>	No Dependencies	
<a href="#">FIA_UAU.6/CA</a>	No Dependencies	
<a href="#">FIA_UID.1/PACE</a>	No Dependencies	
<a href="#">FIA_UID.1/EAC2_Terminal</a>	No Dependencies	
<a href="#">FIA_UAU.4/PACE</a>	No Dependencies	
<a href="#">FIA_UAU.6/PACE</a>	No Dependencies	
<a href="#">FDP_ACF.1/TRM</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FDP_ACC.1/TRM</a>
<a href="#">FDP_ACC.1/TRM</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1/TRM</a>
<a href="#">FDP_UCT.1/TRM</a>	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	<a href="#">FDP_ACC.1/TRM</a> , <a href="#">FTP_ITC.1/PACE</a>
<a href="#">FDP_UIT.1/TRM</a>	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	<a href="#">FDP_ACC.1/TRM</a> , <a href="#">FTP_ITC.1/PACE</a>
<a href="#">FTP_ITC.1/PACE</a>	No Dependencies	
<a href="#">FMT_SMR.1/PACE</a>	(FIA_UID.1)	<a href="#">FIA_UID.1/PACE</a> , <a href="#">FIA_UID.1/EAC2_Terminal</a>
<a href="#">FMT_MTD.1/CVCA_INI</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_MTD.1/CVCA_UPD</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_MTD.1/DATE</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_MTD.1/PA</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_SMF.1</a>

<a href="#">FMT_MTD.1/SK_PICC</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_MTD.1/KEY_READ</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_MTD.1/Initialize_PIN</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_MTD.1/Resume_PIN</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_MTD.1/Change_PIN</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_MTD.1/Unblock_PIN</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_MTD.3</a>	(FMT_MTD.1)	<a href="#">FMT_MTD.1/CVCA_INI</a> , <a href="#">FMT_MTD.1/CVCA_UPD</a> , <a href="#">FMT_MTD.1/DATE</a>
<a href="#">FMT_MTD.1/INI_ENA</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_MTD.1/INI_DIS</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1/PACE</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FTP_ITC.1/CA2</a>	No Dependencies	
<a href="#">FMT_LIM.1</a>	No Dependencies	
<a href="#">FMT_LIM.2</a>	No Dependencies	
<a href="#">FPT_EMS.1</a>	No Dependencies	
<a href="#">FPT_FLS.1</a>	No Dependencies	
<a href="#">FPT_PHP.1</a>	No Dependencies	
<a href="#">FPT_PHP.3</a>	No Dependencies	
<a href="#">FPT_TST.1</a>	No Dependencies	
<a href="#">FMT_SMR.1</a>	(FIA_UID.1)	<a href="#">FIA_UID.1</a>
<a href="#">FMT_SMF.1</a>	No Dependencies	
<a href="#">FMT_MOF.1</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_MSA.1/Admin</a>	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FDP_ACC.1/Signature Creation</a> , <a href="#">FDP_ACC.1/SVD Transfer</a> , <a href="#">FDP_ACC.1/SCD/SVD Generation</a> , <a href="#">FDP_ACC.1/SCD Import</a>
<a href="#">FMT_MSA.1/Signatory</a>	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a> , <a href="#">FDP_ACC.1/Signature Creation</a>

<a href="#">FMT_MSA.2</a>	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_MSA.1/Admin</a> , <a href="#">FMT_MSA.1/Signatory</a> , <a href="#">FDP_ACC.1/Signature Creation</a> , <a href="#">FDP_ACC.1/SCD/SVD Generation</a>
<a href="#">FMT_MSA.3</a>	(FMT_MSA.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_MSA.1/Admin</a> , <a href="#">FMT_MSA.1/Signatory</a>
<a href="#">FMT_MSA.4</a>	(FDP_ACC.1 or FDP_IFC.1)	<a href="#">FDP_ACC.1/Signature Creation</a> , <a href="#">FDP_ACC.1/SCD/SVD Generation</a>
<a href="#">FMT_MTD.1/Admin</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FMT_MTD.1/Signatory</a>	(FMT_SMF.1) and (FMT_SMR.1)	<a href="#">FMT_SMR.1</a> , <a href="#">FMT_SMF.1</a>
<a href="#">FIA_UID.1</a>	No Dependencies	
<a href="#">FIA_AFL.1</a>	(FIA_UAU.1)	<a href="#">FIA_UAU.1</a>
<a href="#">FIA_UAU.1</a>	(FIA_UID.1)	<a href="#">FIA_UID.1</a>
<a href="#">FDP_SDI.2/DTBS</a>	No Dependencies	
<a href="#">FDP_SDI.2/Persistent</a>	No Dependencies	
<a href="#">FDP_RIP.1</a>	No Dependencies	
<a href="#">FDP_ACC.1/Signature Creation</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1/Signature Creation</a>
<a href="#">FDP_ACF.1/Signature Creation</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FMT_MSA.3</a> , <a href="#">FDP_ACC.1/Signature Creation</a>
<a href="#">FCS_COP.1</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	<a href="#">FCS_CKM.4</a> , <a href="#">FCS_CKM.1</a> , <a href="#">FDP_ITC.1/SCD</a>
<a href="#">FCS_CKM.4</a>	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	<a href="#">FCS_CKM.1</a> , <a href="#">FDP_ITC.1/SCD</a>
<a href="#">FCS_CKM.1</a>	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	<a href="#">FCS_COP.1</a> , <a href="#">FCS_CKM.4</a>
<a href="#">FDP_ACC.1/SVD Transfer</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1/SVD Transfer</a>
<a href="#">FDP_ACF.1/SVD Transfer</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FMT_MSA.3</a> , <a href="#">FDP_ACC.1/SVD Transfer</a>
<a href="#">FDP_ACC.1/SCD/SVD Generation</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1/SCD/SVD Generation</a>
<a href="#">FDP_ACF.1/SCD/SVD Generation</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FMT_MSA.3</a> , <a href="#">FDP_ACC.1/SCD/SVD Generation</a>
<a href="#">FTP_ITC.1/SCD</a>	No Dependencies	
<a href="#">FDP_UCT.1/SCD</a>	(FDP_ACC.1 or FDP_IFC.1) and	<a href="#">FTP_ITC.1/SCD</a> , <a href="#">FDP_ACC.1/SCD Import</a>

	(FTP_ITC.1 or FTP_TRP.1)	
<a href="#">FDP_ITC.1/SCD</a>	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	<a href="#">FMT_MSA.3</a> , <a href="#">FDP_ACC.1/SCD Import</a>
<a href="#">FDP_ACC.1/SCD Import</a>	(FDP_ACF.1)	<a href="#">FDP_ACF.1/SCD Import</a>
<a href="#">FDP_ACF.1/SCD Import</a>	(FDP_ACC.1) and (FMT_MSA.3)	<a href="#">FMT_MSA.3</a> , <a href="#">FDP_ACC.1/SCD Import</a>
<a href="#">FTP_ITC.1/SVD</a>	No Dependencies	
<a href="#">FDP_DAU.2/SVD</a>	(FIA_UID.1)	<a href="#">FIA_UID.1</a>
<a href="#">FIA_API.1</a>	No Dependencies	
<a href="#">FDP_UIT.1/DTBS</a>	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	<a href="#">FDP_ACC.1/Signature Creation</a> , <a href="#">FTP_ITC.1/DTBS</a>
<a href="#">FTP_ITC.1/VAD</a>	No Dependencies	
<a href="#">FTP_ITC.1/DTBS</a>	No Dependencies	

**Table 12 SFRs Dependencies**

**Rationale for the exclusion of Dependencies**

**The dependency FMT\_MSA.3 of FDP\_ACF.1/TRM is discarded.** The access control TSF according to FDP\_ACF.1/TRM uses security attributes that have been defined during personalization, and that are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT\_MSA.1 and FMT\_MSA.3) is necessary.

**9.3.3.2 SARs Dependencies**

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

**Table 13 SARs Dependencies**

 IDEMIA	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>126/142</b>
--	--	---

### **9.3.4 Rationale for the Security Assurance Requirements**

The assurance level for this Security Target is EAL5 augmented. EAL5 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL5 is appropriate for commercial products that can be applied to moderate to high security functions. Augmentation results from the selection of:

AVA\_VAN.5 Advanced methodical vulnerability analysis

ALC\_DVS.2 Sufficiency of security measures

#### **9.3.4.1 AVA\_VAN.5 Advanced methodical vulnerability analysis**

The TOE is intended to function in a variety of signature creation systems for qualified electronic signatures. Due to the nature of its intended application, i.e., the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD\_Secrecy, OT.Sigy\_SigF and OT.Sig\_Secure.

#### **9.3.4.2 ALC\_DVS.2 Sufficiency of security measures**

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. Due to the nature of the TOE, there is a need to justify the sufficiency of these procedures to protect the confidentiality and the integrity of the TOE. The TOE shall be protected in confidentiality and integrity during its development to meet the security objective OT.Lifecycle\_Security.

## 10 TOE Summary Specification

---

### 10.1 TOE Summary Specification

This section provides a summary of the security functions implemented by the TOE in order to fulfil the security functional requirements. The summary is structured in security functions.

The security functionalities concerning the IC and the JC Platform are described in [ST-IC], [ST-PL] and are not redefined in this security target, although they must be considered for the TOE.

#### 10.1.1 Chip security functionalities

The full list of the IC Platform security functionalities can be checked in the IC Platform Security Target [ST-IC].

#### 10.1.2 Platform security functionalities

The full list of the JC Platform security functionalities can be checked in the JC Platform Security Target [ST-PL].

#### 10.1.3 Application security functionalities

### SF.AUTHENTICATION

Only authenticated terminals can get access to the user data stored on the TOE. The ID.me applet offers several authentication schemes enabling to authenticate different roles, such as:

- o The signatory entitled to use the services offered by the card. It is called "User Authentication".
- o The device communicating with the card, to establish a trusted channel (secure messaging) and protect the communication. It is called "Device authentication".
- o The administrator of a service, to administrate some features. It is called "Role authentication".

The **User authentication** is based on the submission of a PIN/password (i.e., knowledge based) or a biometric template (i.e., biometry based).

- o Knowledge based: The Authentication of the user relies on a shared secret (PIN), known by both the holder and the smartcard. The Card holder is authenticated by the means of the VERIFY command. For each SCD separate signatory's RADs (PINs) are assigned. The verification process uses a velocity checking mechanism, thus a remaining tries counter and a maximum error counter are defined for each PIN. If the verification fails, the tries counter is decremented by one and an error status that contains the remaining attempts is returned by the application. When all available tries have failed, the PIN is blocked and can no longer be used. Note that a successful verification of the PIN resets its remaining tries counter to the maximum error counter.
- o Biometry based: The most known biometric kind is the "Fingerprint" or the "Facial recognition". Instead of storing a number for the PIN, the card will store the reference template of the biometry that will be used for the verification.

The **Device Authentication** aims at authenticating both entities willing to communicate and securing the communication between the card and a service provider (it might be a terminal, a server, etc).

- o Authentication Scheme: The smart card implements a mutual authentication scheme. This one relies either on 3DES or AES Cipher block and used to:
  - Authenticate the terminal and the card.
  - Generate two temporary keys that will be further used to compute session keys for the secure messaging in the subsequent commands.
  - Initialize the counter used at each checksum computation.
- o PACE Authentication: PACE establishes Secure Messaging between the ID.me application and a terminal based on weak (short) passwords:
  - Strong session keys are provided independent of the strength of the password.
  - The entropy of the password(s) used to authenticate the terminal can be very low (e.g. 6 digits are sufficient in general).

The detailed specification of the PACE protocol can be found in [ICAO9303]. As opposed to the original context in which PACE is used, i.e., before the application selection, the ID.me application simply considers the PACE protocol as another way to initiate secure messaging with the terminal. In other words, PACE is an access condition that may or may not be required to read or write an object in the file system.

- o EAC2 as defined in [TR03110-2] which consists of two parts:
  - Chip Authentication aims at authenticating the chip and initiates a secure communication channel to communicate. The protocol in Version 2 provides explicit authentication of the chip by verifying the authentication token and implicit authentication of the stored data by performing Secure Messaging using the new session keys.
  - Terminal Authentication protocol uses the secure messaging established by the Chip Authentication Mechanism to protect the confidentiality and integrity of the sensitive data during their transmission from the TOE to the terminal. Therefore, Terminal Authentication can only be performed if Chip Authentication has been successfully executed.

The **Role Authentication** presents the procedure to authenticate an external entity to the card in order to associate to it a specific role (e.g. access rights). Two schemes may be used, relying either on 3DES, AES or RSA Cipher block. The following procedure describes:

- o The cryptographic operation that allows the authentication
- o The specification of the associated role in the card This feature is described in [D14890-2], §7.3.

In ID.me, the Access conditions "Secure Messaging" mandates both a successful terminal authentication and an active secure messaging session. This security function manages authentication failure: when the "highest value in the configurable range of positive numbers fixed by the Administrator" unsuccessful authentication attempts have been met, the TSF shall block the RAD. This security functionality allows the following operations to be performed before the user is authenticated:

- o Identification of the user,
- o Establishing a trusted path between the HID and the TOE,
- o Establishing a trusted channel between the SCA and the TOE,



	<b>Security Target Lite ID.eal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>129/142</b>
---	---	---

- o Establishing a trusted channel between the CGA and the TOE.

## **SF.APP\_CRYPTO**

This SF performs high level cryptographic operations:

- o key generation:
  - SF.APP\_CRYPTO performs RSA key generation of size 1024, 1536, 2048, 2560, 3072 and 4096 bits in conformance with RSA PKCS1 v2.1. Key generation is performed based on random numbers generated by a deterministic RNG,
  - SF.APP\_CRYPTO performs Elliptic curves key generation of size 192,224,256, 320, 384,512 and 521 bits in conformance with ANS X9.62.
  - SF.APP\_CRYPTO performs TDES and AES key generation.
- o Digital signature generation:
  - the signature generation function shall have an access condition based upon previous authentication of user.
  - signature generation by using ECDSA algorithm with cryptographic key sizes of 192,224,256, 320, 384,512 and 521 (provided by the cryptographic library of the Platform).
  - signature generation by using RSA algorithm with cryptographic key sizes of 1024, 1536, 2048, 2560 and 4096 bits (provided by Platform).
- o SCD/SVD key pair consistency check: SF.APP\_CRYPTO performs SCD/SVD consistency check before signature generation by signature generation followed by signature verification. If the signature verification does not match the signature generation, then the key pair is not consistent.
- o Encryption/decryption: SF.APP\_CRYPTO performs TDES and AES in order to achieve encryption and decryption in secure messaging.
- o Integrity verification: SF.APP\_CRYPTO performs ISO/IEC 9797-1 algorithm 3 padding 2 (3DES) or CMAC (AES) in order to achieve message authentication code in secure messaging.
- o Authentication cryptogram creation/verification: SF.APP\_CRYPTO performs the following authentication cryptogram calculation/verification:
  - Mutual authentication based on TDES or AES
  - PACE authentication based on [ICAO9303]
- o Random number generation that meet Class DRG.3 according to AIS20 provided by the Platform (e.g. for PACE authentication mechanism).
- o Data Hashing: SF.APP\_CRYPTO performs SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 in conformance with NIST FIPS PUB 180-2, in order to calculate a hash value.
- o Certificate Calculation and verification.
- o RSA based key decipherment.

All cryptographic functionalities are provided by the platform (see [ST-PL]).

## SF.MANAGEMENT

This SF manages the access to objects (files, directories, data and secrets) stored in the ID.me file system. It also controls write access of initialization, pre-personalization and personalization data. This SF ensures secure management of secrets such as cryptographic keys. It also covers access to keys as well as secure key deletion. This SF controls all the operations relative to the RAD/VAD management, including the Cardholder (signatory) authentication:

- o RAD creation: the RAD is stored and is associated to a maximum successful presentation number (usage counter) and to a maximum error number.
- o VAD verification: the RAD can be accessed only if its format and integrity are correct and if the usage counter has not reached 0. If the RAD is blocked, then it cannot be used anymore until unblocked.
- o RAD ratification counter: The number of authentication attempts is limited by a counter associated to the RAD. The counter is decremented each time the VAD verification fails. The RAD cannot be used any longer if the counter reaches zero.
- o RAD usage counter: the usage counter is decremented each time the RAD is verified successfully. When this counter reaches 0, the RAD cannot be verified anymore.
- o RAD modification: the RAD can be changed by the cardholder (loading a new value). The RAD is managed and stored by the application. The operations on RAD and VAD are performed thanks to services offered by the platform.

This SF manages the security environment of the application and:

- o Maintains the roles (e.g. Signatory, Administrator).
- o Controls if the authentication required for a specific operation has been performed with success.
- o Manages restriction to security function access and to security attribute modification.
- o Ensures that only secure values are accepted for security attributes. This security functionality restricts the ability to perform the function Signature creation SFP to Signatory. This security functionality ensures that only Administrator is authorized to
  - Modify Initialization SFP and Signature creation SFP attributes.
  - Specify alternative default values.

This SF provides the electronic signature application with access control and ensures that the following operations are executed by authorized roles:

- o Export of SVD to CGA.
- o Generation of SCD/SVD pair by the Signatory.
- o Creation of RAD by the Administrator.
- o Signing of DTBS/R by S.Signatory.

This SF manages Session key generation: Session keys are protected in integrity and confidentiality during generation. This SF enforces secure storage of the session keys during generation.

This SF manages Secret destruction: This SF calls the security function of the JC Platform to erase keys.

	<b>Security Target Lite ID.eal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>131/142</b>
---	---	---

This SF manages Secret loading: Loading of a secret is always done by an authorized user through a secure command. This command is accepted only after authentication of the authorized user.

This SF manages Secret transfer: This SF manages the secure transfer of every secret to the crypto processor when used for cryptographic operation.

Access control is enforced by the APDU methods as specified in the interface defined in the functional specification.

### **SF.TRUSTED\_CHANNEL**

This SF realizes a secure communication channel to verify authenticity and integrity as well as securing confidentiality of user data between the TOE and other devices connected.

The ID.me Package performs the following secure messaging tasks with external applications (SCA, HID or CGA) for protection of the communication data as the DTBS, authentication data as the VAD or for ensuring the integrity of the SVD:

- o PACE or mutual authentication or EAC2 authentication used to establish session keys for secure messaging.
- o Encryption and decryption of the transmitted message.
- o MAC generation and verification for secure messaging.
- o ECDH key agreement.
- o Secure hash computation.
- o Random number generation.

This SF manages four modes of secure channel during the personalization phase:

- o No secure messaging
- o Integrity mode
- o Confidentiality mode
- o Integrity and confidentiality mode

### **SF.APP\_INTEGRITY**

This security functionality monitors the integrity of sensitive user data and the integrity of the DTBS/R. The integrity of persistently stored data such as SCD, RAD and SVD is monitored using the platform features (see [ST-PL]). In case of integrity error this TSF will:

- o Prohibit the use of the altered data, and
- o Inform the S.Signatory about integrity error. This TSF also monitors the integrity of the access conditions of created data objects and also ensures that no residual information is available after a RAD update or clearance.

### **SF.RATIF**

A counter is associated to a secret key, to a password and to the VAD, which is used to count the number of unsuccessful authentication attempts. The counter is reinitialized when the authentication is successful. If the counter reaches its maximum value, then the related secret is suspended or blocked and cannot be used anymore until unblocked.

## 10.2 SFRs and TSS

### 10.2.1 SFRs and TSS - Rationale

#### All SSCD parts

#### *Protection of the TSF (FPT)*

**FPT\_EMS.1** is met by SF.APP\_INTEGRITY and SF.MANAGEMENT which ensure secure execution of cryptographic operations on keys.

**FPT\_FLS.1** is met by JC Platform and the IC that ensure that failures in the TSF are detected and that the proper actions (reset, card termination) are taken in order to preserve a secure state of the TOE. It is also met by SF.APP\_INTEGRITY that monitors the integrity of sensitive user data and the integrity of the DTBS/R.

**FPT\_PHP.1** is met by SF.APP\_INTEGRITY, the JC Platform and the IC that ensure that physical tampering of the TOE is detected and that the proper actions (reset, card termination) are taken, so that it can be determined if a physical tampering has occurred.

**FPT\_PHP.3** is met by the JC Platform and the IC that ensures that physical tampering of the TOE is detected and that the proper actions (reset, card termination) in order to protect the TOE. It is also met by SF.APP\_INTEGRITY that monitors the integrity of sensitive data.

**FPT\_TST.1** is met by JC Platform and the IC that performs a set of self-tests at start-up, thus checking the correct operation of the TSF, and that verifies the integrity of the stored executable code before or during its execution and by SF.APP\_INTEGRITY that provides means to verify the integrity of the data stored on the TOE.

#### *Security management (FMT)*

**FMT\_SMR.1** is met by SF.AUTHENTICATION that provides user authentication as administrator or as signatory and by SF.MANAGEMENT that grants to the administrator and to the signatory specific access rights, thus defining roles for the TOE.

**FMT\_SMF.1** requires that the TSF shall be capable of performing the following management functions: (1) Creation and modification of the reference authentication data (RAD), (2) Enabling the signature-creation function, (3) Modification of the security attribute SCD/SVD

	<b>Security Target Lite ID.eal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>133/142</b>
---	---	---

management, SCD operational, (4) Change the default value of the security attribute SCD Identifier, (5) none. This is realized by SF.MANAGEMENT.

**FMT\_MOF.1** is met by SF.MANAGEMENT and SF.AUTHENTICATION that ensures that only authenticated signatory can perform DTBS signature.

**FMT\_MSA.1/Admin** is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE.

**FMT\_MSA.1/Signatory** is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE.

**FMT\_MSA.2** is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE and in particular manages the security attributes.

**FMT\_MSA.3** is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE and in particular manage the security attributes, their initialisation and their access rights.

**FMT\_MSA.4** requires that the TSF shall use the following rules to set the value of security attributes: (1) if S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute 'SCD operational of the SCD' shall be set to 'no' as a single operation; (2) if S.Sigy successfully generates an SCD/SVD pair the security attribute 'SCD operational of the SCD' shall be set to 'yes' as a single operation. This is realized by SF.MANAGEMENT and SF.AUTHENTICATION.

#### **FMT\_MTD.1/Admin**

- o is met by SF.MANAGEMENT that manages the authentication function and ensure that only authenticated administrator can create the RAD.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

#### **FMT\_MTD.1/Signatory**

- o is met by SF.MANAGEMENT that manages the authentication function and ensure that only authenticated signatory can modify the RAD.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

#### *Identification and authentication (FIA)*

#### **FIA\_UID.1**

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.

#### **FIA\_AFL.1**

- o This SFR is met by SF.AUTHENTICATION and SF.MANAGEMENT.
- o This SFR is also met by SF.RATIF that ensures that the RAD is blocked after a defined number of failed successive signatory authentication attempts.

	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>134/142</b>
---	--	---

## FIA\_UAU.1

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.
- o is met by SF.TRUSTED\_CHANNEL that provides a trusted secure messaging with CGA and SCA.

### *User data protection (FDP)*

**FDP\_SDI.2/DTBS** is met by SF.APP\_INTEGRITY, that ensures the integrity of data stored in the TOE, by the JC Platform and the IC that ensure that the proper reaction is taken (reset or card termination) if an integrity error is detected, so that the user knows an error had occurred and that no altered data can be used.

**FDP\_SDI.2/Persistent** is met by SF.APP\_INTEGRITY, that ensures the integrity of data stored in the TOE, by the JC Platform and the IC that ensure that the proper reaction is taken (reset or card termination) if an integrity error is detected, so that the user knows an error had occurred and that no altered data can be used.

**FDP\_RIP.1** is met by SF.MANAGEMENT that ensures erasure of data in FLASH and in RAM (e.g. after the signature creation process), and in particular of SCD, VAD and RAD.

**FDP\_ACC.1/Signature\_Creation** is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that all the access conditions are met before a dedicated operation can be performed, and in particular that only a user authenticated as signatory can perform signature of DTBS loading from an authorized SCA with a RSA key pair whose consistency has been verified, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

**FDP\_ACF.1/Signature\_Creation** is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that all the access conditions are met before a dedicated operation can be performed, and in particular that only a user authenticated as signatory can perform signature of DTBS loading from an authorized SCA with a RSA key pair whose consistency has been verified, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

### *Cryptographic support (FCS)*

## FCS\_COP.1

- o is met by SF.APP\_CRYPTO that provides RSA key pair consistency check.
- o is met by SF.APP\_CRYPTO that provides electronic signature generation compliant with RSA PKCS#1 v2.1.
- o is met by SF.APP\_CRYPTO that provides TDES in CBC mode or AES in CBC mode for encryption and decryption.
- o is met by SF.APP\_CRYPTO that provides ISO/IEC 9797-1 algorithm 3 padding 2 (3DES) or CMAC (AES) for integrity.
- o is met by SF.AUTHENTICATION that provides Symmetric and Asymmetric Mutual Authentications.
- o is met by SF.TRUSTED\_CHANNEL that provides secure messaging with CGA and SCA.

	<b>Security Target Lite IDeal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>135/142</b>
---	--	---

**FCS\_CKM.4** is met by SF.MANAGEMENT, as SF.MANAGEMENT manages the secure destruction of secret, and in particular of the SCD.

**SSCD parts 2, 4 and 5 only**

*Cryptographic support (FCS)*

**FCS\_CKM.1**

- o is met by SF.APP\_CRYPTO that ensures that the TOE generates SCD/SVD cryptographic key pairs.
- o is also met by SF.APP\_CRYPTO, which provides RSA calculation.
- o is also met by SF.MANAGEMENT, which ensures the protection of the keys during generation.

*User data protection (FDP)*

**FDP\_ACC.1/SVD\_Transfer** is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SVD export, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

**FDP\_ACF.1/SVD\_Transfer** is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SVD export, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

**FDP\_ACC.1/SCD/SVD\_Generation** is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user under specific conditions can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD/SVD generation, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

**FDP\_ACF.1/SCD/SVD\_Generation** is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user under specific conditions can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD/SVD generation, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

**SSCD parts 3 and 6 only**

*Trusted path/channels (FTP)*

**FTP\_ITC.1/SCD** is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for SCD Import and by SF.TRUSTED\_CHANNEL, SF.APP\_CRYPTO that



	<b>Security Target Lite IDDeal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>136/142</b>
---	---	---

provide cryptographic means to set up a trusted channel between the TOE and a CSP to protect the exchanged data (SCD) from modification and disclosure.

*User data protection (FDP)*

**FDP\_UCT.1/SCD** is met by SF.AUTHENTICATION and SF.MANAGEMENT that ensure that all the conditions are met before allowing a SCD import and by SF.TRUSTED\_CHANNEL, SF.APP\_CRYPTO that provide cryptographic means to protect the SCD from disclosure during its import.

**FDP\_ITC.1/SCD** is met by SF.AUTHENTICATION and SF.MANAGEMENT that ensure that all the required conditions are met before allowing a SCD import operation.

**FDP\_ACC.1/SCD\_Import** is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD import, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

**FDP\_ACF.1/SCD\_Import** is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD import, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

**SSCD part 4 only**

*Trusted path/channels (FTP)*

**FTP\_ITC.1/SVD** is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for SVD Transfer and by SF.TRUSTED\_CHANNEL, SF.APP\_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a CGA to protect the exchanged data (SVD) from modification and disclosure.

*User data protection (FDP)*

**FDP\_DAU.2/SVD** is met by SF.AUTHENTICATION and SF.TRUSTED\_CHANNEL to ensure that exported SVD to the CGA is authenticated and unmodified.

*Identification and authentication (FIA)*

**FIA\_API.1**

- o The TOE supports RSA calculations in order to generate signatures (SF.APP\_CRYPTO).
- o The TOE supports the establishment of a trusted channel/path based on 3DES or AES mutual authentication with negotiation of symmetric cryptographic keys used for the protection of the communication data with respect to confidentiality and integrity (SF.TRUSTED\_CHANNEL, SF.APP\_CRYPTO).



	<b>Security Target Lite IDEal Citiz v2.3-n embedding ID.me 1.6-n application</b>	Ref.: 2019_2000043199 Page: <b>137/142</b>
---	--	---

**SSCD parts 5 and 6 only**

*User data protection (FDP)*

**FDP\_UIT.1/DTBS** requires that integrity of the DTBS/R to be signed is to be verified, as well as the DTBS/R is not altered by the TOE. This is provided by the trusted channel integrity verification mechanisms (SF.TRUSTED\_CHANNEL, SF.APP\_CRYPTO).

*Trusted path/channels (FTP)*

**FTP\_ITC.1/VAD** is met by SF.AUTHENTICATION, SF.MANAGEMENT that enforce the access right policy for VAD transfer and by SF.TRUSTED\_CHANNEL, SF.APP\_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a HID to protect the exchanged data (VAD) from modification and disclosure.

**FTP\_ITC.1/DTBS** is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for DTBS Import and by SF.TRUSTED\_CHANNEL, SF.APP\_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a SCA to protect the exchanged data (DTBS) from modification and disclosure.

**Additional SFRs related to EAC2**

**FCS\_RND.1**

- o is met by SF.APP\_CRYPTO and SF.AUTHENTICATION.

**FCS\_CKM.1/DH\_PACE**

- o is met by SF.APP\_CRYPTO that ensures that the TOE generates cryptographic key pairs for PACE.
- o is also met by SF.APP\_CRYPTO, which provides DH calculation.
- o is also met by SF.MANAGEMENT, which ensures the protection of the keys during generation.

**FCS\_COP.1/SHA**

- o is met by SF.APP\_CRYPTO that provides Data Hashing.

**FCS\_COP.1/SIG\_VER**

- o is met by SF.APP\_CRYPTO that provides signature verification.

**FCS\_COP.1/PACE\_ENC**

- o is met by SF.AUTHENTICATION that provides PACE authentication, and
- o is met by SF.APP\_CRYPTO that provides TDES in CBC mode or AES in CBC mode for encryption and decryption.
- o is met by SF.TRUSTED\_CHANNEL that provides secure messaging with CGA and SCA.

**FCS\_COP.1/PACE\_MAC**

- o is met by SF.AUTHENTICATION that provides PACE authentication, and
- o is met by SF.APP\_CRYPTO that provides TDES in CBC mode or AES in CBC mode for MAC calculation.
- o is met by SF.TRUSTED\_CHANNEL that provides secure messaging with CGA and SCA.

**FIA\_UAU.1/PACE**

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.
- o is met by SF.TRUSTED\_CHANNEL that provides a trusted secure messaging with CGA and SCA.

**FIA\_UAU.5/PACE**

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.
- o is met by SF.TRUSTED\_CHANNEL that provides a trusted secure messaging with CGA and SCA.

**FIA\_AFL.1/Suspend\_PIN**

- o This SFR is met by SF.AUTHENTICATION and SF.MANAGEMENT.
- o This SFR is also met by SF.RATIF that ensures that the PIN or PUK is suspended after a defined number of failed successive signatory PACE authentication attempts.

**FIA\_AFL.1/Block\_PIN**

- o This SFR is met by SF.AUTHENTICATION and SF.MANAGEMENT.
- o This SFR is also met by SF.RATIF that ensures that the PIN or PUK is blocked after a defined number of failed successive signatory PACE authentication attempts.

**FIA\_AFL.1/PACE**

- o This SFR is met by SF.AUTHENTICATION and SF.MANAGEMENT.
- o This SFR is also met by SF.RATIF that ensures that the PIN, PUK, MRZ or CAN is suspended until the next successful authentication attempt by an configurable amount of time after a defined number of failed signatory PACE authentication attempts.

**FIA\_UAU.1/EAC2\_Terminal**

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.
- o is met by SF.TRUSTED\_CHANNEL that provides a trusted secure messaging with CGA and SCA.

**FIA\_API.1/CA**

- o The TOE supports the establishment of a trusted channel/path based on 3DES or AES mutual authentication with negotiation of cryptographic keys used for the protection of the communication data with respect to confidentiality and integrity (SF.TRUSTED\_CHANNEL, SF.APP\_CRYPTO).

**FIA\_UAU.6/CA**

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.
- o is met by SF.TRUSTED\_CHANNEL that provides a trusted secure messaging with CGA and SCA.

**FIA\_UID.1/PACE**

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.

**FIA\_UID.1/EAC2\_Terminal**

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.

**FIA\_UAU.4/PACE**

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.
- o is met by SF.TRUSTED\_CHANNEL that provides a trusted secure messaging with CGA and SCA.

**FIA\_UAU.6/PACE**

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.
- o is met by SF.TRUSTED\_CHANNEL that provides a trusted secure messaging with CGA and SCA.

**FDP\_ACF.1/TRM**

- o is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user under specific conditions can perform a dedicated operation, and in particular that only users authenticated as authenticated terminal, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

**FDP\_ACC.1/TRM**

- o is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user under specific conditions can perform a dedicated operation, and in particular that only users authenticated as authenticated terminal, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

**FDP\_UCT.1/TRM**

- o is met by SF.AUTHENTICATION and SF.MANAGEMENT that ensure that all the conditions are met before allowing user data transmission and by SF.TRUSTED\_CHANNEL, SF.APP\_CRYPTO that provide cryptographic means to protect user data from disclosure during its import.

**FDP\_UIT.1/TRM** requires that integrity of user data to be authenticated. This is provided by the trusted channel integrity verification mechanisms (SF.TRUSTED\_CHANNEL, SF.APP\_CRYPTO).

**FTP\_ITC.1/PACE**

- o is met is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for data exchange between the TOE and a PACE terminal and by SF.TRUSTED\_CHANNEL, SF.APP\_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a PACE terminal to protect the exchanged data from modification and disclosure.

**FMT\_SMR.1/PACE**

- o is met by SF.AUTHENTICATION that provides user authentication for PACE and by SF.MANAGEMENT that grants to the users specific access rights, thus defining roles for the TOE.

**FMT\_MTD.1/CVCA\_INI**

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated personalization agent can write initial CVCA (public key, meta-data of the certificate, current date).
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

**FMT\_MTD.1/CVCA\_UPD**

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated Country Verifying Certification Authority can update CVCA (public key, meta-data of the certificate).
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

**FMT\_MTD.1/DATE**

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated users (Country Verifying Certification Authority, Document Verifier or EAC2 terminal) can modify the current date of CVCA.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

**FMT\_MTD.1/PA**

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated personalization agent can write SOC and SOD selected in Access Control SFP.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

**FMT\_MTD.1/SK\_PICC**

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated personalization agent can load SKPICC selected in Access Control SFP.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

**FMT\_MTD.1/KEY\_READ**

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that none can read PACE passwords and SKPICC.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

**FMT\_MTD.1/Initialize\_PIN**

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated personalization agent can write PIN, PUK, MRZ and CAN, selected in Access Control SFP.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

**FMT\_MTD.1/Resume\_PIN**

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated electronic document holder can resume suspended PIN selected in Access Control SFP.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

**FMT\_MTD.1/Change\_PIN**

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated users (electronic document holder or an authorized terminal) can change blocked PIN selected in Access Control SFP.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

**FMT\_MTD.1/Unblock\_PIN**

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated users (electronic document holder or an authorized terminal) can unblock blocked PIN selected in Access Control SFP.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

**FMT\_MTD.3**

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only secure values are accepted for TSF data of the Terminal Authentication protocol 2 and the Access Control SFP.

**FMT\_MTD.1/INI\_ENA**

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated Manufacturer can write Initialisation Data and Pre-personalisation Data.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

**FMT\_MTD.1/INI\_DIS**

- o is met by SF.MANAGEMENT that manages the authentication function and ensures that only authenticated Personalisation Agent can read out Initialisation Data and Pre-personalisation Data.
- o is met by SF.AUTHENTICATION that provides the authentication protocol.

**FTP\_ITC.1/CA2**

- o is met is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for data exchange between the TOE and an EAC2 terminal and by SF.TRUSTED\_CHANNEL, SF.APP\_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and an EAC2 terminal to protect the exchanged data from modification and disclosure.

**FMT\_LIM.1**

- o is met by SF.MANAGEMENT and SF.AUTHENTICATION.

**FMT\_LIM.2**

- o is met by SF.MANAGEMENT and SF.AUTHENTICATION.