CardOS® DI V5.4

Security Target 'CardOS DI V5.4 QES Version 1.0'

Revision 1.61R

Edition 04/2020

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

The reproduction, transmission or use of this document or its contents is not permitted without express written authority. Offenders will be liable for damages. All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Atos Information Technology GmbH
Otto-Hahn-Ring 6

D-81739 Munich
Germany

Disclaimer of Liability

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

Subject to change without notice
© Atos Information Technology GmbH 2020

CardOS is a registered trademark of Atos Information Technology GmbH.

Contents

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

Revision History

Version	Date	Remarks
1.61R	2020-04-17	Release Version

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

1 Scope

This Security Target defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation, the Information Technology security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria evaluation and provides

- the ST introduction in 4 Security Target Introduction (ASE_INT),
- the Conformance claims in 5 Conformance Claims (ASE_CCL),
- the Security problem definition in 6 Security Problem Definition (ASE_SPD),
- the Security objectives in 7 Security Objectives (ASE_OBJ),
- the Extended components definition in 8 Extended Components Definition (ASE_ECD),
- the Security and assurance requirements in 9 Security Requirements (ASE_REQ),
- the Rationale in 9.3 Security Requirements Rationale and
- the TOE summary specification in 10 TOE Summary Specification (ASE_TSS).

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

prEN 419211-1, Protection profiles for secure signature creation device – Part 1: Overview[1]

ISO/IEC 15408-1:2009[2] Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

ISO/IEC 15408-2[2], Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components

ISO/IEC 15408-3[2], Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components

[1] To be published. This document was submitted to the Enquiry procedure under reference prEN 14169-1.

[2] ISO/IEC 15408-1, -2 and -3 respectively correspond to Common Criteria for Information Technology Security Evaluation, Parts 1, 2 and 3.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

3 Conventions and Terminology

3.1 Conventions

The content and structure of this document follow the rules and conventions laid out in ISO/IEC 15408-1.

Normative aspects of content in this European Standard are specified according to the Common Criteria rules and not specifically identified by “shall”.

3.2 Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

3.2.1 Legislative references

This European Standard reflects the requirement of a European Directive in the technical terms of a protection profile. The following terms are used in the text to reference this Directive:

3.2.1.1 eIDAS

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 199/93/EC*” [EU-Reg-910-2014]

Note 1 to entry: References in this document to a specific article and paragraph of Regulation (EU) No 910/2014 are of the form “(**eIDAS:** n.m)”.

Note 2 to entry: Directive 1999/93/EC of the European Parliament and of the Council (**the Directive**), dealt with electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. Regulation (EU) No 910/2014 enhances and expands the acquis of **the Directive**.

3.2.1.2 the Directive

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on “*a Community framework for electronic signatures*” [DIR-1999/93/EC]

Note 1 to entry: References in this document to a specific article and paragraph of Directive 1999/93/EC are of the form “(**the Directive:** n.m)”.

Note 2 to entry: According to **eIDAS**, **the Directive** is repealed with effect from 1 July 2016. References to the repealed Directive shall be construed as references to **eIDAS**.

3.2.2 Technical Terms

Note 1 to entry: ***Bold and cursive*** term indicates that this part is added to contents of PP [BSI-PP0059-2009] and [CC-Part1-V3.1] as well as to **eIDAS** and **the Directive** .

(1) administrator

user who performs TOE initialization, TOE personalization, AQES update, or other TOE administrative functions

Note 1 to entry: “AQES update” added to content, as term for summarizing TOE administrative functions that may be performed by the administrator during the Phase “Usage/Operational”, see also “***application qualified electronic signature update (AQES update)***”.

(2) advanced electronic seal

electronic seal, which meets the requirements set out in **eIDAS: 3.26**

Note 1 to entry: According to **eIDAS article 36** an advanced electronic seal shall meet the following requirements:

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

(a) it is uniquely linked to the creator of the seal;

(b) it is capable of identifying the creator of the seal;

(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and

(d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

(3) advanced electronic signature

electronic signature which meets specific requirements in **eIDAS: 3.11**

Note 1 to entry: According to **eIDAS article 26** an electronic signature qualifies as an advanced electronic signature if:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

(4) application qualified electronic signature update (AQES update)

summary of TOE administrative functions that may be performed by the administrator during the Phase "Usage/Operational", such as:

(a) generation of SCD/SVD pair,

(b) export of SVD,

(c) creation/update of EFs / DFs, e.g. import of certificate info.

(5) authentication

an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed (**eIDAS: 3.5**)

(6) authentication data

information used to verify the claimed identity of a user

(7) body governed by public law

body defined in point (4) of Article 2(1) of **the Directive** (**eIDAS: 3.8**)

(8) card holder (CH)

a person who holds (and is a legitimate user) of an SSCD, see also signatory

(9) certificate

digital signature used as electronic attestation binding signature verification data to a person confirming the identity of that person as legitimate signer (**the Directive: 2.9**)

(10) certificate for electronic seal

an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person (**eIDAS: 3.29**)

(11) certificate for electronic signature

an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person (**eIDAS: 3.14**)

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

(12) certificate for website authentication

an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued (**eIDAS: 3.38**)

(13) certificate info

information associated with an SCD/SVD pair that may be stored in a secure signature creation device

Note 1 to entry: Certificate info may include:

(a) a signer's public key certificate, or

(b) 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, or

(c) a public key certificate as defined in X.509.

Note 2 to entry: Certificate info may contain information to allow the user to distinguish between several certificates.

(14) certificate generation application (CGA)

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

(15) certification service provider (CSP)

entity that issues certificates or provides other services related to electronic signatures (**the Directive: 2.11**)

(16) common criteria (CC)

set of rules and procedures for evaluating the security properties of a product

Note 1 to entry: see bibliography for details on the specification of Common Criteria.

(17) conformity assessment body

a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides (**eIDAS: 3.18**)

(18) creator of a seal

a legal person who creates an electronic seal (**eIDAS: 3.24**)

(19) data to be signed (DTBS)

all of the electronic data to be signed including a user message and signature attributes

(20) data to be signed or its unique representation (DTBS/R)

data received by a secure signature creation device as input in a single signature creation operation

Note 1 to entry: Examples of DTBS/R are:

(a) a hash value of the data to be signed (DTBS), or

(b) an intermediate hash value of a first part of the DTBS complemented with a remaining part of the DTBS, or

(c) the DTBS.

(21) electronic document

any content stored in electronic form, in particular text or sound, visual or audiovisual recording (**eIDAS: 3.35**)

(22) electronic identification

the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person (**eIDAS: 3.1**)

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

(23) electronic identification means

a material and/or immaterial unit containing person identification data and which is used for authentication for an online service (**eIDAS: 3.2**)

(24) electronic identification scheme

a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons (**eIDAS: 3.4**)

(25) electronic registered delivery service

a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations (**eIDAS: 3.36**)

(26) electronic seal

data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity (**eIDAS: 3.25**)

(27) electronic seal creation data

unique data, which is used by the creator of the electronic seal to create an electronic seal (**eIDAS: 3.28**)

(28) electronic seal creation device

configured software or hardware used to create an electronic seal (**eIDAS: 3.31**)

(29) electronic signature

data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign (**eIDAS: 3.10**)

(30) electronic signature creation data

unique data which is used by the signatory to create an electronic signature (**eIDAS: 3.13**)

(31) electronic signature creation device

configured software or hardware used to create an electronic signature (**eIDAS: 3.22**)

(32) electronic time stamp

data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time (**eIDAS: 3.33**)

(33) evaluation assurance level (EAL)

a set of assurance requirements for a product, its manufacturing process and its security evaluation specified by Common Criteria

(34) legitimate user

user of a secure signature creation device who gains possession of it from an SSCD-provisioning service provider and who can be authenticated by the SSCD as its signatory

(35) mass signature

The generation of more than one signature at a time after suitable authentication, e.g. for an automated process

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

(36) notified body

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 this standard and for determining admissible algorithms and algorithm parameters (**the Directive:** 1.1b and 3.4)

(37) person identification data

a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established (**eIDAS: 3.3**)

(38) product

hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services (**eIDAS: 3.21**)

(39) protection Profile (PP)

document specifying security requirements for a class of products that conforms in structure and content to rules specified by common criteria

(40) public sector body

a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate (**eIDAS: 3.7**)

(41) qualified certificate

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** of **the Directive** (**the Directive: 2.10**)

(42) qualified certificate for electronic seal

a certificate for electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III of **eIDAS** (**eIDAS: 3.30**)

(43) qualified certificate for electronic signature

a certificate for electronic seals, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of **eIDAS** (**eIDAS: 3.15**)

(44) qualified certificate for website authentication

a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV of **eIDAS** (**eIDAS: 3.39**)

(45) qualified electronic registered delivery service

an electronic registered delivery service which meets the requirements laid down in Article 44 of **eIDAS** (**eIDAS: 3.37**)

(46) qualified electronic seal

an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal (**eIDAS: 3.27**)

(47) qualified electronic seal creation device

an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II of **eIDAS** (**eIDAS: 3.32**)

(48) qualified electronic signature

an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures (**eIDAS: 3.12**)

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

(49) qualified certificate for electronic seal

a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III of **eIDAS** (**eIDAS: 3.30**)

(50) qualified electronic signature creation device

an electronic signature creation device that meets the requirements laid down in Annex II of **eIDAS** (**eIDAS: 3.23**)

Note 1 to entry This is the definition taken from **eIDAS** which correlates with the definition of secure signature creation device (**SSCD**) from **the Directive**

(51) qualified electronic time stamp

an electronic time stamp which meets the requirements laid down in Article 42 of **eIDAS** (**eIDAS: 3.34**)

(52) qualified trust service

a trust service that meets the applicable requirements laid down in **eIDAS** (**eIDAS: 3.17**)

(53) qualified trust service provider

a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body (**eIDAS: 3.20**)

(54) reference authentication data (RAD)

data persistently stored by the TOE for authentication of the signatory

(55) relying party

a natural or legal person that relies upon an electronic identification or a trust service (**eIDAS: 3.6**)

(56) registration authority (RA)

an organizational entity acting under the security policy of the ***trust center***. The (local or remote) **RA** is often locally separated from a ***trust center***.

(57) secure signature creation device (SSCD)

a signature creation device which meets the requirements laid down in *Annex III of* **the Directive** (**the Directive: 2.5 and 2.6**)

Note 1 to entry: An SSCD may be evaluated according to the security target conforming to a PP as defined in the series of European Standards.

Note 2 to entry: a signature-creation device can also be used as a seal creation device and therefore SSCD is an acronym for secure signature (and seal) creation device.

(58) security target (ST)

document specifying security requirements for a particular product that conforms in structure and content to rules specified by common criteria, which may be based on one or more Protection Profiles

(59) signatory

a person who holds (and is a legitimate user) of an SSCD and acts either on their own behalf or on behalf of the natural or legal person or entity they represent

(60) signature attributes

Additional information that is signed together with a user message

(61) signature creation application (SCA)

application complementing an SSCD with a user interface with the purpose to create an electronic signature

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Note 1 to entry: A signature creation application is software consisting of a collection of application components configured to:

(a) present the data to be signed (DTBS) for review by the signatory,

(b) obtain prior to the signature process a decision by the signatory,

(c) if the signatory indicates by specific unambiguous input or action its intent to sign send a DTBS/R to the TOE

(d) process the electronic signature generated by the SSCD as appropriate, e.g. as attachment to the DTBS.

(62) signature creation data (SCD)

unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature (**the Directive: 2.4**)

Note 1 to entry: For the PPs of this standard the SCD is held in the SSCD.

(63) signature creation system (SCS)

complete system that creates an electronic signature consisting of an SCA and an SSCD

(64) signature verification data (SVD)

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

(65) signature verification device

configured software or hardware used to implement the signature verification data (SVD) (**the Directive: 2.8**)

(66) signed data object (SDO)

electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.

(67) SSCD-provisioning service

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

(68) StartKey

is needed for the protection of card commands and is changed from the secret factory value to a known value with a command sequence provided by the TOE software developer.

(69) target of evaluation (TOE)

abstract reference in a document, such as a Protection Profile, for a particular product that meets specific security requirements

(70) TOE security functions (TSF)

functions implemented by the TOE to meet the requirements specified for it in a Protection Profile or Security Target

(71) trust center

an organizational entity which may comprise of the entities Initialization Service, Personalization Service, Certification Authority acting as Certification Service Provider and Registration Authority, all acting under the trust center's security policy.

(72) trust service

an electronic service normally provided for remuneration which consists of: (**eIDAS: 3.16**)

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

(b) the creation, verification and validation of certificates for website authentication; or

(c) the preservation of electronic signatures, seals or certificates related to those services;

(73) trust service provider

a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider (**eIDAS: 3.19**)

(74) user

entity (human user or external IT entity) outside the TOE that interacts with the TOE

(75) user message

data determined by the signatory as the correct input for signing

(76) validation

the process of verifying and confirming that an electronic signature or a seal is valid (**eIDAS: 3.41**)

(77) validation data

data that is used to validate an electronic signature or an electronic seal (**eIDAS: 3.40**)

(78) verification authentication data (VAD)

data input to an SSCD for authentication of the signatory

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

3.3 Abbreviated Terms

AQES	**A**pplication **Q**ualified **E**lectronic **S**ignature
CA	**C**hip **A**uthentication
CAN	**C**ard **A**ccess **N**umber
CC	**C**ommon **C**riteria[3]
CGA	**C**ertificate **G**eneration **A**pplication
CH	**C**ard **H**older
CPM	**C**hip **M**anufacturer
CSP	**C**ertificate **S**ervice **P**rovider
DTBS	**D**ata **T**o **B**e **S**igned
DTBS/R	**D**ata **T**o **B**e **S**igned or its unique **R**epresentation
EAL	**E**valuation **A**ssurance **L**evel[3]
ES	**E**mbedded **S**oftware
HID	**H**uman **I**nterface **D**evice
IC	**I**ntegrated **C**ircuit
IT	**I**nformation **T**echnology
PACE	**P**assword **A**uthenticated **C**onnection **E**stablishment
PP	**P**rotection **P**rofile[3]
PP SSCD KG	**P**rotection **P**rofile for **S**ecure **S**ignature **C**reation **D**evice with **K**ey **G**eneration
PP SSCD KG TCCGA	**P**rotection **P**rofile for **S**ecure **S**ignature **C**reation **D**evice with **K**ey **G**eneration and **T**rusted **C**ommunication with **C**ertificate **G**eneration **A**pplication
PP SSCD KG TCSCA	**P**rotection **P**rofile for **S**ecure **S**ignature **C**reation **D**evice with **K**ey **G**eneration and **T**rusted **C**ommunication with **S**ignature **C**reation **A**pplication
RA	**R**egistration **A**uthority
RAD	**R**eference **A**uthentication **D**ata
RC	**R**etry **C**ounter
SCA	**S**ignature **C**reation **A**pplication
SCD	**S**ignature **C**reation **D**ata
SCS	**S**ignature **C**reation **S**ystem
SDO	**S**igned **D**ata **O**bject
SFP	**S**ecurity **F**unction **P**olicy
SFR	**S**ecurity **F**unctional **R**equirement
SSCD	**S**ecure **S**ignature (and seal) **C**reation **D**evice
ST	**S**ecurity **T**arget[3]
SVD	**S**ignature **V**erification **D**ata
TC	**T**rusted **C**ommunication
TOE	**T**arget **O**f **E**valuation[3]
TSF	**T**OE **S**ecurity **F**unctionality[3]
VAD	**V**erification **A**uthentication **D**ata

[3] See Bibliography [CC-Part1-V3.1], [CC-Part2-V3.1], [CC-Part3-V3.1] for details on the specification of Common Criteria.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

4 Security Target Introduction (ASE_INT)

4.1 ST Reference

Title	Security Target 'CardOS DI V5.4 QES Version 1.0'
Revision	1.61R
Author	Atos Information Technology GmbH
General Status	Release
Publication date	04/2020
Registration	BSI-DSZ-CC-1112
CC Version	3.1, Revision 5
Assurance Level	The assurance level for this ST is EAL4 augmented

This Security Target claims conformance on the following protection profiles covering a number of requirements for a secure signature creation device:

Part 2: Device with key generation, [BSI-CC-PP-0059-2009-MA-02] (**PP SSCD KG**)[4]

Part 4: Extension for device with key generation and trusted communication with certificate generation application, [BSI-CC-PP-0071-2012-MA-01] (**PP SSCD KG TCCGA**)[5]

Part 5: Extension for device with key generation and trusted communication with signature creation application, [BSI-CC-PP-0072-2012-MA-01] (**PP SSCD KG TCSCA**)[6]

Protection profiles PP SSCD KG, PP SSCD KG TCCGA and PP SSCD KG TCSCA are established by CEN as a European standard for products to create electronic signatures. They fulfill requirements of directive[7] 1999/93/EC [DIR-1999/93/EC] of the European parliament and of the council of 13 December 1999 on a community framework for electronic signatures.

In accordance with article 9 of this European directive this standard can be indicated by the European commission in the Official Journal of the European Communities as generally recognized standard for electronic signature products.

The core protection profile *PP SSCD KG* defines security functional requirements and security assurance requirements that comply with those defined in Annex III of the Directive[8] for a secure signature creation device (SSCD). This secure signature creation device is the target of evaluation (TOE) for protection profile *PP SSCD KG*.

European Union Member States may presume that there is compliance with the requirements laid down in Annex III of the Directive[9] when an electronic signature product is evaluated to a Security Target (ST) that is compliant with protection profile *PP SSCD KG*.

PP SSCD KG describes core security requirements for a secure device that can **generate** a signing key[10] (signature creation data, SCD) and operates to create electronic signatures with the generated key. A device evaluated according to *PP SSCD KG* and used in the specified environments can be trusted to create any type of digital signature. As such *PP SSCD KG* can be used for any device that has been configured to create a digital signature. Specifically *PP SSCD KG* allows the qualification of a product as a device for creating a qualified electronic signature as defined in **the Directive**.

[4] Strict conformance is claimed for both configurations **TC-SCA-Mandatory** and **TC-SCA-CL-Only**.

[5] Strict conformance is claimed for both configurations **TC-SCA-Mandatory** and **TC-SCA-CL-Only**.

[6] For the configuration **TC-SCA-Mandatory** strict conformance is claimed; for the configuration **TC-SCA-CL-Only** the additions apply only for the contactless communication interface.

[7] This European directive is referred to in the ST as “the Directive”.

[8] Also complies with security functional requirements and security assurance requirements defined in Annex II of eIDAS**.**

[9] Also complies with the requirements laid down in Annex II of eIDAS**.**

[10] An SSCD that can generate its own SCD/SVD was defined in the previous version of PP SSCD KG (CWA14169) as a Type 3 SSCD. The notion of types does not exist anymore in this series of ENs.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

When operated in a secure environment for signature creation a signer may use an SSCD that fulfills only these core security requirements to create an advanced electronic signature.[11]

PP SSCD KG TCCGA is an extension and conforms[12] to the core *PP SSCD KG*. It defines the security requirements for a trusted communication to a certificate generation application (CGA). These security features allow a changed life cycle of the TOE, i.e. the signatory may generate an SCD/SVD key pair suitable to create qualified electronic signatures and transfer the corresponding public key (signature verification data, SVD) as input to the CGA **after** the delivery of the SSCD. The TOE supports its authentication as SSCD by the CGA of the Certification service provider (CSP) and a trusted communication with this CGA for protection of the SVD.

PP SSCD KG TCSCA is an extension and conforms[13] to the core *PP SSCD KG*. It defines the security requirements for an SSCD used in environments, where the communication between SSCD and the signature creation application (SCA) is assumed to be protected by the SSCD and the SCA. These security features allow using the TOE in a more complex operational environment. The TOE supports a trusted communication with an SCA for protection of authentication data and data to be signed.

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

PP SSCD KG TCCGA is marginalized with **CGA**

PP SSCD KG TCSCA is marginalized with **SCA**

In addition, margins **PACE** or **CA**, respectively, are applied, when large text passages concern the PACE or Chip Authentication (CA) functionality.

Note:

1. The PACE and Chip Authentication functionality is only applicable in cases where the communication between the TOE and another entity via trusted channel is mandatory, such as:
    a. For the communication between the TOE and SCA for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.
    b. For the communication between the TOE and an administrative entity (CGA or SSCD Issuing Application) in the life cycle Phase “Usage/Operational”.

4.2 TOE Reference

This ST refers to the TOE 'CardOS DI V5.4 QES Version 1.0' developed by Atos Information Technology GmbH.

[11] An advanced electronic signature is defined as an electronic signature created by an SSCD using a public key with a public key certificate created as specified in **the Directive**.

[12] See [CC-Part1-V3.1] for the usage of multiple protection profiles.

[13] See [CC-Part1-V3.1] for the usage of multiple protection profiles.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

4.3 TOE Overview

1. TOE type

The TOE 'CardOS DI V5.4 QES Version 1.0' is intended to be used as secure signature creation device (SSCD) in accordance with **eIDAS,** so the TOE consists of the part of the implemented software related to the generation of qualified electronic signatures in combination with the underlying hardware ('Composite Evaluation'). The hardware and the software of the TOE is determined by the components listed in chapter 4.4.4 Components of the TOE.

The underlying platform of the TOE is a Smart Card Integrated Circuit (SCIC), which can be used as wafer, module, smart card ("card" for short). The SCIC already contains the OS "CardOS DI V5.4" when delivered.

The TOE as defined by this Composite Security Target consists of

- the Infineon chip (SCIC) SLE78CLFX*P* (M7892 Design Steps D11 and G12) and the libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010,
- the OS "CardOS DI V5.4" and
- the Application QES.

The Infineon chip (SCIC) SLE78CLFX*P* (M7892 Design Steps D11 and G12) and the libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010 are certified, see [Infineon-ST-M7892-D11-G12] and [BSI-DSZ-CC-0891].

SLE78CLFX*P* (M7892 Design Steps D11 and G12) is an abbreviation and denotes dual interface chips (design steps D11 and G12) which differ only in flash size and input capacity (of the contactless interface):

- SLE78CLFX4000P(H) with 404kByte flash, 27pF
- SLE78CLFX408AP(H) with 404kByte flash, 78pF
- SLE78CLFX400BP(H) with 404kByte flash, 78pF

The chips can be packaged in the modules M8.4, MCC8, MCS8 (27pF) or COM8.6, COM 10.6 (78pF) or other modules or packages.

Please note that all these derivatives are covered by the certificate [BSI-DSZ-CC-0891].

Usage and major security features of the TOE
CardOS DI V5.4 is a fully interoperable ISO 7816 compliant multi-application smart card operation system, including a cryptographic library enabling the user to generate high security electronic signatures based on ECDSA with a key length of up to 521 bit and RSA with a key length of up to 3072 bit.

Beside contact based communication according Part 3 of ISO/IEC 7816-3 [ISO-IEC-7816-part-3] CardOS DI V5.4 supports contactless communication according ISO/IEC 14443 [ISO-IEC-14443-2018]. The TOE 'CardOS DI V5.4 QES Version 1.0' can be configured for sole contact based communication, sole contactless communication and for dual interface supporting contact based and contactless communication.

The TOE 'CardOS DI V5.4 QES Version 1.0' allows generation of cryptographically strong signatures over previously externally or internally calculated hash values including last round hashing. It is possible to personalize the TOE 'CardOS DI V5.4 QES Version 1.0' in a way that the TOE 'CardOS DI V5.4 QES Version 1.0' can generate **single** or **mass** signatures[14] according to **eIDAS**. The TOE 'CardOS DI V5.4 QES Version 1.0' generates the signature key pair (SCD/SVD). The TOE 'CardOS DI V5.4 QES Version 1.0' is able to protect the secrecy of the internally generated and stored signature creation data (SCD), i.e. secret key and restricts its usage to the authorized signatory only. This restriction on usage is done via the well-known PIN authentication mechanism.

The TOE 'CardOS DI V5.4 QES Version 1.0' supports the following methods:

PACE according to [BSI-TR-03110-1-V220], [BSI-TR-03110-2-V221], [ICAO-TR-110] for

- the identification and authentication of the user as the legitimate card holder
- the establishment of a trusted channel between the terminal and the card
- the protection against tracking and eavesdropping

The TOE 'CardOS DI V5.4 QES Version 1.0' provides the following secrets to be used within the PACE protocol (PIN.QES assigns an additional password for authentication to create qualified electronic signatures):

[14] Mass signature generation is used to create either a limited or unlimited number of electronic signatures in a row for an automated process.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Secret	Minimum length	Initial value set by	Used to authenticate for
PIN.CH	6 digits	Signatory on first usage	qualified electronic signature creation[15], verification of PIN.QES, change reference data of PIN.QES[16] and change reference data of PIN.CH
PUK.CH (optional)	8 digits	Signatory on first usage or administrator on personalization	reset retry counter of PIN.CH, reset retry counter of PIN.QES, reset retry counter of PIN.T, change reference data of PIN.CH and change reference data of PUK.CH
PIN.T	5 digits	Administrator on personalization	activation of PUK.CH (if present), activation of PIN.QES
CAN	6 digits	Administrator on personalization	Verification of PIN.QES, change reference data of PIN.QES[16] and unblock PIN.CH, PUK.CH (if present) and PIN.ADMIN
PIN.ADMIN	24 digits	Administrator on personalization	verification of PIN.QES, signature key generation[17], export of SVD, certificate import and key termination[18]

Table 4-1: Secrets used within the PACE protocol

PIN.ADMIN and CAN are only used as shared passwords for the PACE authentication method.

PIN.T, PIN.CH and the optional PUK.CH

a) must be used as shared passwords for the PACE authentication method for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.

b) can be used as shared passwords for the PACE authentication method **or** as PINs for the PIN authentication mechanism for the configuration TC-SCA-CL-Only for contact-based communication only.

Note:

1 For the TOE 'CardOS DI V5.4 QES Version 1.0' PIN.CH is only used as shared password for the PACE authentication method. However additional applications may use PIN.CH as PIN for the PIN authentication mechanism. This is only possible for the configuration TC-SCA-CL-Only for contact-based communication. Using PIN.CH as PIN is beyond the scope of this ST.

PIN.CH, PUK.CH, PIN.T and PIN.ADMIN are protected against denial-of-service attacks when used where a trusted channel establishment is mandatory.

- For PIN.CH, PUK.CH and PIN.T this applies for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.
- For PIN.ADMIN this always applies for all communication interfaces.

The protection against denial-of-service attacks is achieved by setting the chip into a **suspended state**, before the retry counter of the secret in question is exhausted after consecutive failed authentication attempts. Before the very last retry to authenticate against PIN.CH, PUK.CH, PIN.T or PIN.ADMIN, respectively, can be done, an authentication against **CAN** must be performed.

Chip Authentication Version 1 according to [BSI-TR-03110-1-V220] for

- proof of the authenticity of the chip to the terminal (e.g. CGA)
- the establishment of a trusted channel between the terminal and the card

[15] Additionally requires verification of PIN.QES

[16] Additionally requires verification of PIN.QES

[17] Additionally requires verification of PIN.QES

[18] Additionally requires verification of PIN.QES

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

The Application QES is designed for the creation of legally binding qualified electronic signatures and qualified electronic seals as defined in **eIDAS**. It offers one signature key for the creation of **qualified electronic signatures/seals**.

To create an electronic signature, the legitimate user must authenticate himself against the **RAD**, which consists of one or more secrets stored on the chip. The RAD also ensures that the SSCD is in a non-operational state when delivered to the signatory. In the Phase “Usage/Preparation” (see also section 4.4.3) the transport PIN (PIN.T), PIN.CH, CAN and optionally PUK.CH are set in the personalization step and delivered to the signatory. The creation of a qualified electronic signature is additionally protected by the secret **PIN.QES**, which is a password with a minimum length of 6 digits stored on the chip. For PIN.QES and optionally PUK.CH no initial values are set in the Phase “Usage/Preparation”. The secrets must be activated by the signatory on first usage. For the disabling of the transport protection and activating the secrets the authentication against the transport PIN (PIN.T) is required.

In order to use the SCD for advanced signature creation the signatory has to be authenticated using PIN.QES. The conditional establishment of a trusted channel can be done using either[19]

(a) PIN.CH **or**

(b) CAN

Beside the files for the Application QES there may be additional files for other applications, e.g. for an ID application, which do not belong to the TOE. Each application, in particular the Application QES, can define access rules to protect itself against misuse and unauthorized access. Usually the data structures for applications are loaded onto the card during initialization and personalization. Nevertheless it is still possible to add data structures of additional applications during the Phase “Usage/Operational”. These data structures do not include any executable code; therefore application functionality is always limited to the functionality of the operating system.

The adding of data structures of additional applications during the Phase “Usage/Operational” is only possible after establishing a trusted channel using Chip Authentication following PACE authentication using PIN.ADMIN as the shared password. In the Phase “Usage/Preparation” (see also section 4.4.3) PIN.ADMIN is set in the personalization step and only known to the administrator.

Configurations
In order to meet customer requirements, it is possible to configure the TOE 'CardOS DI V5.4 QES Version 1.0' in various configurations during TOE initialization and TOE personalization. These differ in the requirement for **Trusted Channel establishment via PACE Authentication** for the communication between the TOE and the signature creation application (SCA), dependent on the communication interface used. The differences in the configurations are realized by different access rule settings for the appropriate objects and cannot be changed in Phase “Usage/Operational” of the TOE. The configurations are:

No.	Configuration-ID	Description
1	**TC-SCA-Mandatory**	For **strict** conformance according to **PP SSCD KG TCSCA** for all communication interfaces, meaning the TOE and the SCA **must** communicate through a trusted channel for all communication interfaces. For **strict** conformance according to **PP SSCD KG TCCGA** for all communication interfaces, meaning the TOE and the CGA **must** communicate through a trusted channel for all communication interfaces[20].
2	**TC-SCA-CL-Only**	The TOE and the SCA **must** communicate through a trusted channel for **contactless communication** only (as required by **PP SSCD KG TCSCA)** and **may** communicate through a trusted channel for **contact-based communication**. For **strict** conformance according to **PP SSCD KG TCCGA** for all communication interfaces, meaning the TOE and the CGA **must** communicate through a trusted channel for all communication interfaces[21].

Table 4-2: Available TOE configurations

[19] Applies for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only

[20] The TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.

[21] The TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Apart from that, different variants within the configurations are possible, e.g. **single** or **mass** signature creation. The variants are determined through the use of the appropriate personalization scripts (cf. 4.4.4 Components of the TOE) or through other personalization processes that guarantee the same result. Further details are given in [Atos-V54DI-QES-Adm-Guid].

The following applies for variants without PUK.CH:

- If the Signatory cannot remember his PIN.CH or PIN.QES, a new PIN value cannot be set for either PIN.
- If PIN.T, PIN.CH or PIN.QES of the Signatory is blocked, it is not possible to unblock either of them.

The following applies for variants with PUK.CH:

- If the Signatory cannot remember his PIN.QES, a new PIN value cannot be set for it.
- If the Signatory cannot remember his PIN.CH, the Signatory uses PUK.CH to set a new PIN value.
- If PIN.T, PIN.CH or PIN.QES of the Signatory is blocked, the Signatory uses PUK.CH to unblock the blocked PIN.
- If the Signatory cannot remember his PUK.CH, a new PUK value cannot be set for it.
- If PUK.CH of the Signatory is blocked or its use counter is zero, it is not possible to unblock it or to set the use counter to a new value.

Note:

1. If PUK.CH is present, the PUK has a finite use counter.

3. Required non-TOE hardware/software/firmware

The SCIC on which the TOE 'CardOS DI V5.4 QES Version 1.0' bases conforms to ISO 7816 and needs the usual IT environment for such smart cards, i.e. a signature creation application (SCA) on the host connected with a smart card terminal.

4. Optional Non-TOE software

An SCIC product containing the TOE 'CardOS DI V5.4 QES Version 1.0' may contain further applications, besides the Application QES, e.g. for electronic identity documents.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

4.4 TOE Description

In the following the TOE 'CardOS DI V5.4 QES Version 1.0' is described according the Protection profiles for Secure signature creation devices [BSI-CC-PP-0059-2009-MA-02], [BSI-CC-PP-0071-2012-MA-01] and [BSI-CC-PP-0072-2012-MA-01].

4.4.1 Operation of the TOE

This section presents a functional overview of the TOE 'CardOS DI V5.4 QES Version 1.0' and its distinct operational environments (Figure 4-1 and Figure 4-2).

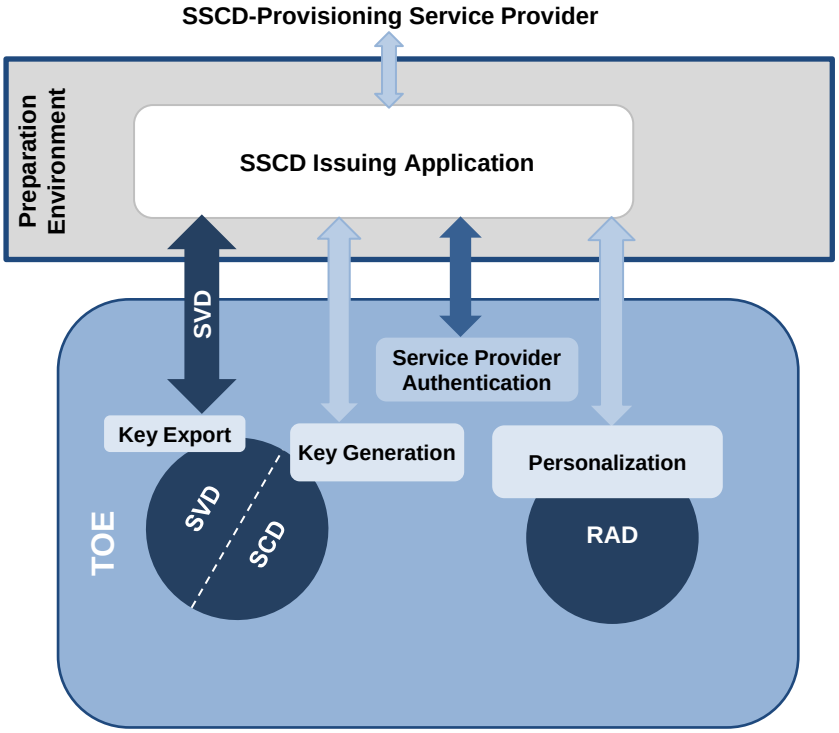

Figure 4-1: SSCD functions and operational environments within the **Phase "Usage/Preparation"**

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

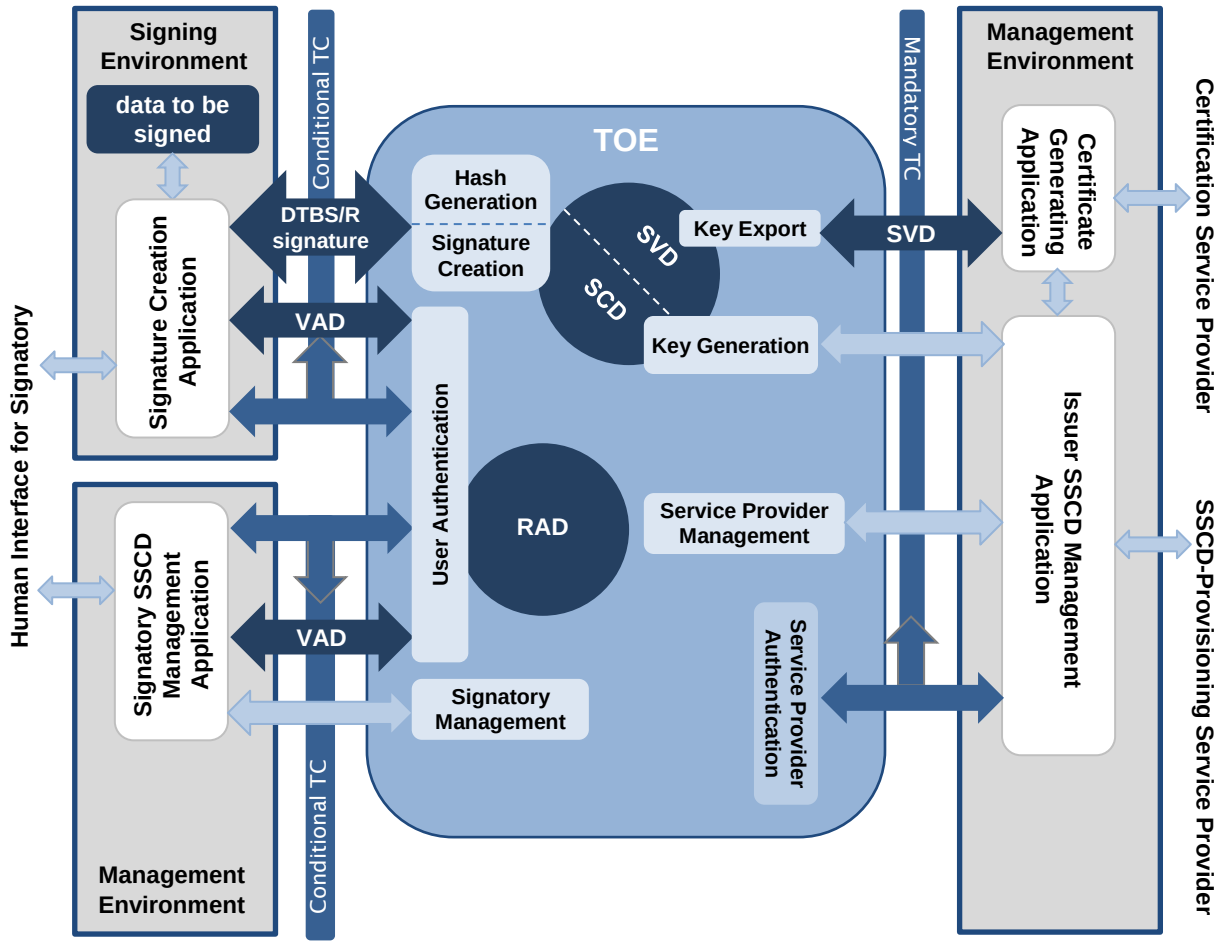

Figure 4-2: SSCD functions and operational environments including trusted channels for communication within the **Phase "Usage/Operational"**

The TOEs interactions comprise of:

- **Preparation environment**

  In this environment the TOE 'CardOS DI V5.4 QES Version 1.0' interacts during the Phase "Usage/Preparation" with a SSCD-provisioning service provider through a SSCD issuing application to personalize the TOE 'CardOS DI V5.4 QES Version 1.0' with personal information of the legitimate user, generate the signature key pair on the card and export the for the signature verification data (SVD) corresponding with signature creation data (SCD) the TOE has generated.

- **Signing environment:**

  In this environment the TOE 'CardOS DI V5.4 QES Version 1.0' interacts with a signer through a signature creation application (**SCA**) to sign data after authenticating the signer as its signatory. The **SCA** 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[22].

SCA The TOE 'CardOS DI V5.4 QES Version 1.0' conditionally[23] provides the functionality to communicate with the **SCA** through a trusted channel to ensure the integrity of the **DTBS** respective **DTBS/R** and the confidentiality and integrity of the **VAD** received from the HID as needed by the user authentication method.

- **Management environments**

[22] At a pure functional level the **SSCD** creates an electronic signature or electronic seal respectively; for an implementation of the **SSCD**, in that meeting the requirements of **PP SSCD KG** and with the key certificate created as specified in Annex I and Annex III of **eIDAS**, the result of the signing process can be used as to create a qualified electronic signature or qualified electronic seal respectively.

[23] Applies for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

In this environment the TOE 'CardOS DI V5.4 QES Version 1.0' interacts with

- the signatory through a signatory SSCD management application to perform management operations, e.g. to reset a blocked **RAD**.

SCA The TOE 'CardOS DI V5.4 QES Version 1.0' conditionally[24] provides the functionality to communicate with the signatory SSCD management application through a trusted channel to ensure the confidentiality and integrity of the **VAD** received from the HID as needed by the user authentication method.

- an SSCD-provisioning service provider through an issuer SSCD management application to perform management operations, e.g. generate the signature key pair on the card and store certificate info to the **SSCD**.

  The TOE 'CardOS DI V5.4 QES Version 1.0' provides the functionality to communicate with the issuer SSCD management application through a trusted channel to ensure the confidentiality and integrity of the data presented to the **SSCD**.

- a certification service provider (CSP) through a certificate generation application (CGA) to obtain a certificate for the signature verification data (SVD) corresponding with signature creation data (SCD) the TOE has generated.

CGA The TOE 'CardOS DI V5.4 QES Version 1.0' provides the functionality to export the **SVD** through a trusted channel allowing the **CGA** to check the authenticity of the **SVD**[25].

The TOE stores signature creation data and reference authentication data (RAD, i.e PIN.QES). The TOE protects the confidentiality of the SCD and restricts its use in signature creation to its signatory. The digital signature created with the TOE is a *qualified electronic signature* as defined in **eIDAS** if the certificate for the SVD is a qualified certificate (Annex I of **eIDAS**). Determining the state of the certificate as qualified is beyond the scope of EN 419211.

The SCA is assumed to 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 value 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.

SCA The TOE and the SCA conditionally[26] communicate through a trusted channel in order to protect the integrity of the DTBS/R.

The TOE stores signatory RAD to authenticate a user as its signatory. The TOE protects the confidentiality and integrity of the RAD. The TOE receives the VAD from the SCA. If the signature creation application handles requesting obtaining a VAD from the user, it is assumed to protect the confidentiality and integrity of this data.

Note 3: Within the PACE protocol, not the VAD (i.e. the password for PIN.CH, PUK.CH, PIN.T, PIN.ADMIN or CAN, respectively) is transmitted from the terminal to the TOE, but a nonce encrypted with the VAD (zero-knowledge protocol).

A SSCD-provisioning service provider interacts 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 may include:

- initializing the transport PIN (PIN.T), PIN.CH, CAN, PIN.ADMIN and optionally the PUK;
- generating a key pair;
- exporting the SVD from the TOE;
- storing personal information of the legitimate user.

A certification service provider (CSP) and a SSCD-provisioning service provider interact with the TOE in the secure management environment to perform different administrative functions of the TOE after control of the TOE is given to the legitimate user. These functions may include:

- generating a key pair;
- exporting the SVD from the TOE;

[24] Applies for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only

[25] The TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.

[26] Applies for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

- storing certificate info.

CGA 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[27].

The TOE 'CardOS DI V5.4 QES Version 1.0' is a smart card. A smart card terminal may 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, after presenting the document to the user and after obtaining the authorization PIN initiates the electronic signature creation function of the smart card through the terminal.

4.4.2 Target of Evaluation

The TOE is a combination of hardware and software configured to securely create, use and manage signature creation data (SCD). The SSCD protects the SCD during its whole life cycle as to be used in a signature creation process 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:

a) to generate signature creation data (SCD) and the correspondent signature verification data (SVD),

CGA b) to export the **SVD** for certification through a trusted channel to the **CGA**,

CGA c) to prove the identity as **SSCD** to external entities,

d) to, optionally, receive and store certificate info,

e) to switch the TOE from a non-operational state to an operational state, and

f) if in an operational state,

i. to create a **single** digital signature for data with the following steps:

1) present the data to be signed (DTBS) to the signatory correctly, whereas this function is provided by the TOE environment,

2) authenticate the signatory and determine its intent to sign,

SCA 3) receive data to be signed or a unique representation thereof (DTBS/R) or the intermediate value + remainder of DTBS (last round hashing) conditionally[28] through a trusted channel from SCA,

4) optionally apply an appropriate hash function to the DTBS,

5) apply an appropriate cryptographic signature creation function using the SCD to the DTBS/R.

ii. to create a **limited** number of digital signatures in a row for an automated process with the following steps:

1) determine the signatory's its intent to start the limited mass signing process,

2) authenticate the signatory,

SCA 3) receive data to be signed or a unique representation thereof (DTBS/R) or the intermediate value + remainder of DTBS (last round hashing) conditionally[29] through a trusted channel from SCA,

4) optionally apply an appropriate hash function to the DTBS,

5) apply an appropriate cryptographic signature creation function using the SCD to the DTBS/R.

6) and stop signing if the number of signatures exceeds the limit or authorization of the signatory is withdrawn.

iii. to create an **unlimited** number of digital signatures in a row for an automated process with the following steps:

1) determine the signatory's its intent to start the unlimited mass signing process,

2) authenticate the signatory,

SCA 3) receive data to be signed or a unique representation thereof (DTBS/R) or the intermediate value + remainder of DTBS (last round hashing) conditionally[30] through a trusted channel from SCA,

4) optionally apply an appropriate hash function to the DTBS,

[27] The TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase "Usage/Operational".

[28] Applies for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only

[29] Applies for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only

[30] Applies for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

5) apply an appropriate cryptographic signature creation function using the SCD to the DTBS/R.
6) and stop signing if the authorization of the signatory is withdrawn.

The TOE is prepared for the signatory's use by

a) generating the SCD/SVD pair, and
b) personalizing for the signatory by storing in the TOE:
   1) authentication data (i.e. PIN.T) for the signatory to be able to activate the RAD
   2) optionally, personal unblocking key (i.e. PUK.CH) for the signatory to be able to unblock the RAD
   3) optionally, certificate info for the SCD in the TOE.

After preparation the SCD is in a non-operational state. Upon receiving a TOE the signatory shall verify its non-operational state and change the SCD state to operational by activating the RAD.

As the initial value of the RAD is set by the legitimate user, the verification authentication data (VAD) required for use of the TOE in signing is implicitly known only by the legitimate user. After preparation he must be informed of the transport PIN (PIN.T) value enabling him to activate (and set) the RAD. The means of providing this information is expected to protect the confidentiality and the integrity of the transport PIN (PIN.T).

If the use of an SCD is no longer required, then it shall be destroyed by erasing the SCD data as well as the associated certificate info, if any exists.

4.4.3 TOE Life Cycle

4.4.3.1 General

The TOE life cycle distinguishes phases for development, preparation and operational use.

The development stage and production stage of the TOE together constitute the development phase of the TOE. The development phase is subject of CC evaluation according to the assurance life cycle (ALC) class. The development phase ends with the delivery of the TOE from the CPM. The delivery of the TOE from the CPM is considered the delivery in the sense of CC.

The delivery of the TOE to an SSCD provisioning service provider may be done directly from the CPM or by taking a detour through the stock of the TOE developer and some distributors.

The operational usage of the TOE comprises the Phase "Usage/Preparation" and the Phase "Usage/Operational". In the Phase "Usage/Preparation" the initialization and personalization of the TOE is done. In this phase the personal information of the legitimate user is written, the SCD/SVD pair is generated and optionally the SVD is exported to CSP and the according certificate info is imported. The Phase "Usage/Operational" begins when the signatory has obtained the TOE and the transport PIN (PIN.T). Enabling the TOE for signing requires the SCD/SVD pair stored in its memory[31].

The life cycle (Figure 4-3[32]) allows the generation of an SCD/SVD pair before as well as after the delivery to the signatory.

[31] Note that according to **PP SSCD KG** the Phase "Usage/Operational" begins before the Phase "Usage/Preparation" ends, because the signatory must enable the SCD for use (by setting the VAD) after receiving the TOE and the transport PIN (PIN.T).

[32] the asterisks * marks the optional import of the certificate info during TOE preparation and certificate info deletion when SCD is destroyed.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

The TOE life cycle as SSCD ends when the SCD in it has been rendered permanently unusable. Rendering a SCD in the SSCD unusable may include deletion of the any stored corresponding certificate info.

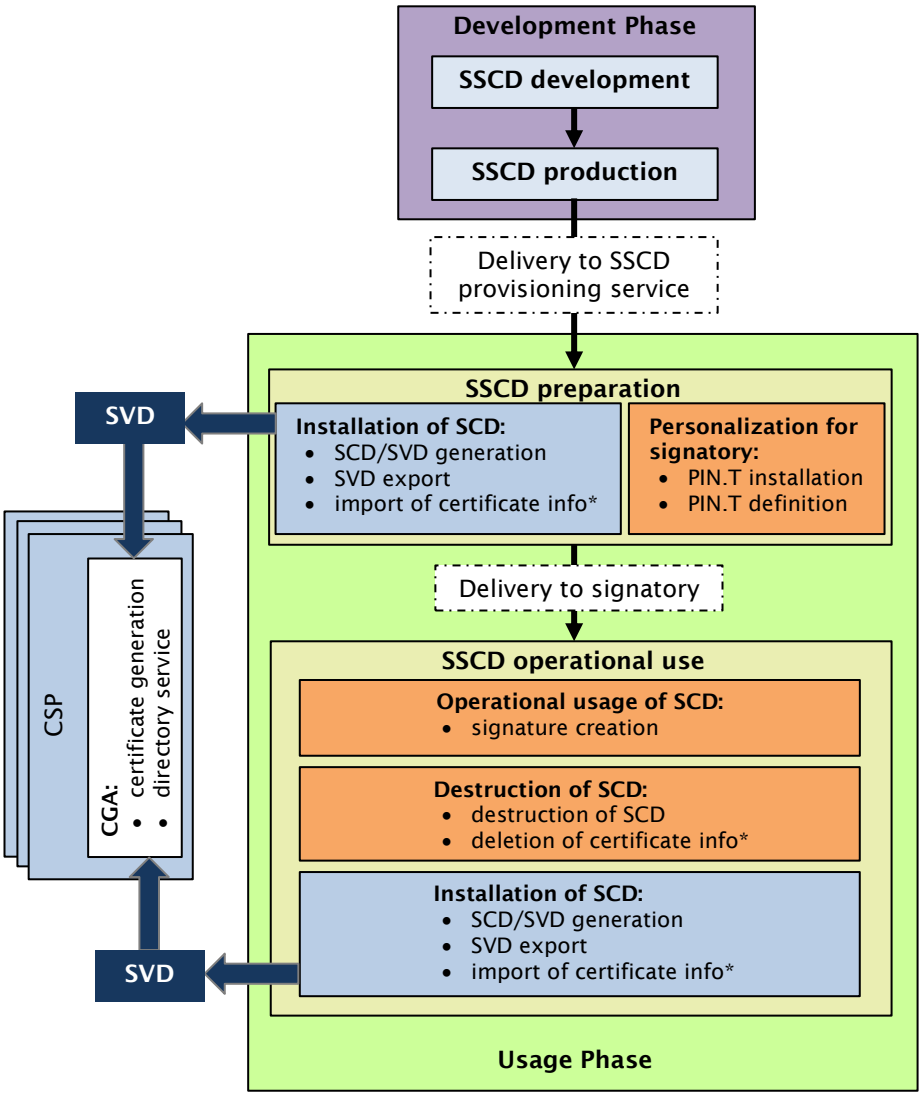

Figure 4-3: Example of TOE life cycle based on [BSI-CC-PP-0059-2009-MA-02], 4.3.3 TOE lifecycle, Figure 1 – Example of TOE lifecycle

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

4.4.3.2 Phase "Usage/Preparation"

An SSCD-provisioning service provider having accepted the TOE from a manufacturer prepares the TOE for use and delivers it to its legitimate user. The Phase "Usage/Preparation" ends when the legitimate user has received the TOE from the SSCD-provisioning service and any SCD it might already hold have been enabled for use in signing.

During preparation of the TOE, as specified above, an SSCD-provisioning service provider performs the initialization and personalization of the TOE, which includes the following tasks:

CGA a) Initialize the security functions in the TOE for the identification as SSCD, for the proof of this SSCD identity to external entities, and for the protected export of the SVD (required by **PP SSCD KG TCCGA**). [33]

b) Obtain information on the intended recipient of the device as required for the preparation process and for identification as a legitimate user of the TOE.

c) Set the transport PIN (PIN.T) to enable the legitimate user to activate the RAD and prepare information about the transport PIN (PIN.T) value for delivery to the legitimate user.

d) Optionally, set PUK.CH to enable the legitimate user to unblock the RAD and the transport PIN (PIN.T) and prepare information about the PUK.CH value for delivery to the legitimate user[34].

e) Generate a certificate for the SCD by (more details about the **SVD certification task** are given below):

   1) the TOE generating an SCD/SVD pair and obtaining a certificate for the SVD exported from the TOE, or

   2) initializing security functions in the TOE for protected export of the SVD and obtaining a certificate for the SVD after receiving a protected request from the TOE.

f) Optionally, present certificate info to the SSCD.

CGA g) Link the identity of the TOE as SSCD and the identity of the legitimate user as potential applicant for certificates for SVD generated by the TOE (required by **PP SSCD KG TCCGA**).

h) Deliver the TOE, the accompanying transport PIN (PIN.T) info, PIN.CH info and optionally the personal unblocking key (PUK.CH) info to the legitimate user.

The **SVD certification task** of an SSCD-provisioning service provider as specified in **PP SSCD KG** may support a centralized, pre-issuing key generation process, with the SCD generated before delivery to the legitimate user. Additionally, that task may support SCD generation by the signatory after delivery and outside the secure preparation environment (decentralized). The TOE supports both key generation processes, for example with the SCD generated centrally and later regenerated by the administrator in the Phase "Usage/Operational" after expiration of the (qualified) certificate for the corresponding SVD. The TOE provides a trusted channel to the CGA protecting the integrity of the SVD[35].

Data required for inclusion in the SVD certificate at least includes (Annex I of **eIDAS**):

- the SVD which correspond to SCD under the control of the signatory;
- the name of the signatory or a pseudonym, which is to be identified as such;
- an indication of the beginning and end of the period of validity of the certificate.

The data included in the certificate may have been stored in the SSCD during personalization.

Before initiating the actual certificate signature the CGA verifies the sender and the SVD received from the TOE by:

a. establishing the sender as genuine SSCD and the identity of the TOE as SSCD,
b. establishing the integrity of the SVD to be certified as sent by the originating SSCD,
c. establishing that the originating SSCD has been personalized for the applicant for the certificate as legitimate user,
d. establishing the correspondence between SCD implemented in the SSCD and the received SVD, and
e. an assertion that the signing algorithm and key size for the SVD are approved and appropriate for the type of certificate.

The proof of correspondence between an SCD stored in the TOE and an SVD may be implicit in the security mechanisms applied by the CGA. Security requirements to protect the SVD export function and the certification data if the SVD is generated by the signatory and then exported from the SSCD to the CGA are specified in this ST.

Prior to generating the certificate the certification service provider (CSP) shall assert the identity of the signatory

[33] This task is only necessary in case a communication channel to the CGA (via trusted channel) in the Life Cycle Phase "Usage/Operational" is needed.

[34] PUK.CH may be absent or if present may be set by the signatory during activation of the RAD.

[35] The TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase "Usage/Operational".

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

specified in the certification request as the legitimate user of the TOE.

If the TOE is used for creation of qualified or advanced electronic signatures, the certificate links the signature verification data to the person (i.e. the signatory) and confirms the identity of that person (**the Directive: 2.9**).

4.4.3.3 Phase “Usage/Operational”

In this life cycle phase the signatory can use the TOE to create qualified or advanced electronic signatures.

The Phase “Usage/Operational” begins when the signatory has obtained the TOE and the transport PIN (PIN.T). Enabling the TOE for signing requires the SCD to be stored in its memory.

The signatory can also interact with the SSCD through a trusted channel to perform management tasks, e.g. reset a RAD value or use counter if the PIN in the reference data has been lost or blocked. Such management tasks require a secure environment, which can be achieved by interacting through a trusted channel[36].

The signatory can render an SCD in the TOE permanently unusable. Rendering the last SCD in the TOE permanently unusable ends the life of the TOE as SSCD.

CGA In the usage phase, SCD/SVD generation by the TOE and SVD export from the TOE may take place in the Phase “Usage/Preparation” (by the SSCD-provisioning service provider) and in the Phase “Usage/Operational” (together by the SSCD-provisioning service provider and the signatory). The TOE provides a trusted channel to the CGA protecting the integrity of the SVD[37]. For a key generated by the signatory he may be allowed to choose some of the data in the certificate request for instance to use a pseudonym instead of the legal name in the certificate[38]. If the conditions to obtain a qualified certificate are met the new key can also be used to create advanced electronic signatures.

The optional TOE functions for additional key generation and certification in the Phase “Usage/Operational” require additional security functions in the TOE and an interaction with the SSCD-provisioning service provider or certification service provider (CSP) through a trusted channel.

CGA Before generating the certificate including the SVD exported from the TOE, the CGA additionally establishes

a) the identity of the TOE as SSCD,
b) that the originating SSCD has been personalized for the applicant for the certificate as legitimate user, and
c) the correspondence between SCD stored in the SSCD and the received SVD.

The TOE life cycle as SSCD ends when all set of SCD stored in the TOE are destructed. This may include deletion of the corresponding certificates.

4.4.3.4 Mapping of PP's SSCD life cycle onto TOE's life cycle

The TOE provides other notations for the life cycle than the example in Figure 4-3.

The following table maps these TOE's life cycle phases, [Atos-V54-CardOS-Users-Manual] "Card Life Cycle Phases", onto the SSCD example life cycles of [BSI-CC-PP-0059-2009-MA-02]:

TOE life cycle phases	SSCD example life cycle phases
./.	Development Phase
MANUFACTURING	Usage Phase
ADMINISTRATION	
OPERATIONAL[39]	
DEATH	

Table 4-3: Mapping of TOE life cycle phases to PP’s SSCD life cycle phases

[36] Applies for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only

[37] The TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.

[38] The certificate request in this case will contain the name of the signatory as the requester, as for instance it may be signed by the signatory’s existing SCD.

[39] After the TOE has been switched to phase OPERATIONAL (permanently), it is only possible to temporarily switch to phase ADMINISTRATION. After a reset the TOE is always in (its permanent) phase OPERATIONAL.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

Note:

1. CardOS V5.4 User's Manual, [Atos-V54-CardOS-Users-Manual], lists in section "Card Life Cycle Phases" two additional phases: "PHYSINIT" and "PHYSPERS". These two phases do not concern this TOE, because these phases deal with CardOS DI V5.4 personalization images.

MANUFACTURING is the phase after chip production and provides an implicit authentication of the administrator. It represents the start of TOE initialization which comprises the following tasks:

- performing of acceptance procedures,
- card authentication by changing the StartKey,
- creation of the MF and
- start-up in the CC terminology.

After the creation of the MF the TOE switches to phase ADMINISTRATION.

Phase ADMINISTRATION represents the TOE initialization and TOE personalization which comprises all the tasks performed by an SSCD-provisioning service provider during preparation of the TOE (see 4.4.3.2 Phase "Usage/Preparation").

Notes:

1. During phase ADMINISTRATION the TOE is switched to phase OPERATIONAL. After the TOE has been (permanently) switched to phase OPERATIONAL it is only possible to switch it temporarily to phase ADMINISTRATION. In this sense ADMINISTRATION can be seen rather as a state than as a life cycle phase of the TOE. After a reset the TOE is always in phase OPERATIONAL.
2. Some initialization, personalization tasks require the TOE to be in ADMINSTRATION. After the TOE has been switched to phase OPERATIONAL prior, the TOE is only switched temporarily to phase ADMINSTRATION until switched back explicitly or implicitly via reset.
3. The switch to phase OPERATIONAL during phase ADMINISTRATION is necessary in order to perform the TOE initialization and TOE personalization by two different entities where a re-authentication of the administrator using the symmetric authentication mechanism with the Administrator Personalization Key is necessary.

Phase OPERATIONAL represents the PP's SSCD life cycle phase "SSCD Operational use" (see 4.4.3.3 Phase "Usage/Operational") which begins when the signatory has obtained the TOE. It comprises

(a) Activation of Application QES (by signatory)

(b) Using the signature creation function (by signatory)

(c) Optional update of Application QES (by SSCD-provisioning service provider or certification service provider (CSP))

(d) Optional destruction of the SCD (by signatory)[40]

Notes:

1. The Application QES is activated by setting the RAD and thus disabling the transport protection
2. The TOE administrative functions for updating the Application QES comprises generation of SCD/SVD pair, export of SVD, creation/update of EFs / DFs, e.g. import of certificate info.

The TOE life cycle ends with the life cycle phase DEATH in which the SCD is permanently blocked.

[40] As stated in 4.4.3.3 Phase "Usage/Operational", the signatory can render an SCD in the TOE permanently unusable. Rendering the last SCD in the TOE permanently unusable ends the life of the TOE as SSCD.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

4.4.4 Components of the TOE

The components of the TOE are

1. **Hardware:** SLE78CLFX*P* (M7892 Design Steps D11 and G12)
2. **Software:** CardOS DI V5.4 for 404kByte flash with the Infineon libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010
3. **Configuration scripts:** for TOE initialization, TOE personalization and AQES update
4. **Manuals:** CardOS V5.4 User's Manual [Atos-V54-CardOS-Users-Manual] and CardOS DI V5.4 Package & Release Notes [Atos-V54DI-CardOS-PR-Notes]
5. **Security Target:** Security Target 'CardOS DI V5.4 QES Version 1.0', this document
6. **Guidance:** Administrator Guidance 'CardOS DI V5.4 QES Version 1.0' [Atos-V54DI-QES-Adm-Guid], User Guidance 'CardOS DI V5.4 QES Version 1.0' [Atos-V54DI-QES-User-Guid] and Application QES Description 'CardOS DI V5.4 QES Version 1.0' [Atos-V54DI-QES-AQES]

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

5 Conformance Claims (ASE_CCL)

5.1 CC Conformance Claim

This ST claims conformance to the Common Criteria version 3.1 Release 5:

- Part 1 [CC-Part1-V3.1],
- Part 2 [CC-Part2-V3.1] extended, and
- Part 3 [CC-Part3-V3.1] conformant.

5.2 PP Claim, Package Claim

The conformance claims of this ST are dependent on the configuration used. Two configurations are available: **TC-SCA-Mandatory** and **TC-SCA-CL-Only**.

For the configuration **TC-SCA-Mandatory** strict conformance to the following Common Criteria protection profiles is claimed:

"Protection profiles for Secure signature creation device – Part 2: Device with key generation", BSI-CC-PP-0059-2009-MA-02 [BSI-CC-PP-0059-2009-MA-02]

CGA "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-MA-01 [BSI-CC-PP-0071-2012-MA-01]

SCA "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-MA-01 [BSI-CC-PP-0072-2012-MA-01]

For the configuration **TC-SCA-CL-Only** strict conformance to the following Common Criteria protection profiles is claimed:

"Protection profiles for Secure signature creation device – Part 2: Device with key generation", BSI-CC-PP-0059-2009-MA-02 [BSI-CC-PP-0059-2009-MA-02]

CGA "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-MA-01 [BSI-CC-PP-0071-2012-MA-01]

Additionally for the configuration **TC-SCA-CL-Only** the Common Criteria protection profile [BSI-CC-PP-0072-2012-MA-01] is taken to secure the communication between TOE and SCA through a trusted channel for the contactless communication interface only. No strict conformance is claimed, since the communication between TOE and SCA through a trusted channel is optional for the contact-based communication interface.

This ST is conforming to assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [CC-Part3-V3.1].

5.3 Conformance Rationale

This ST claims conformance to **PP SSCD KG**, **PP SSCD KG TCCGA** and **PP SSCD KG TCSCA**[41].

CGA SCA This implies for this ST:

a) The security problem definition (SPD) for **PP SSCD KG**, **PP SSCD KG TCCGA** and **PP SSCD KG TCSCA** are described by the same threats, organizational security policies and assumptions.

[41] For the configuration **TC-SCA-Mandatory** strict conformance is claimed; for the configuration **TC-SCA-CL-Only** the additions only apply for the contactless communication interface.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

b) The security objectives for the TOE include all the security objectives for the TOE of **PP SSCD KG** and in addition:

1) OT.TOE_SSCD_Auth (Authentication proof as SSCD) defined in **PP SSCD KG TCCGA**[42]

2) OT.TOE_TC_SVD_Exp (Trusted channel for SVD) defined in **PP SSCD KG TCCGA**[43]

3) OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import) defined in **PP SSCD KG TCSCA**

4) OT.TOE_TC_DTBS_Imp (Trusted channel for DTBS) defined in **PP SSCD KG TCSCA**

c) The security objectives for the operational environment include all the security objectives for the TOE of **PP SSCD KG** and in addition:

1) OE.CGA_SSCD_Auth (Pre-initialization of the TOE for SSCD authentication) defined in **PP SSCD KG TCCGA**[44]

2) OE.CGA_TC_SVD_Imp (CGA trusted channel for SVD import) defined in **PP SSCD KG TCCGA**[45]

Furthermore, the following modifications are performed:

1) **PP SSCD KG TCCGA** substitutes OE.SSCD_Prov_Service (Authentic SSCD provided by SSCD-provisioning service) by OE.Dev_Prov_Service.[46]

2) **PP SSCD KG TCSCA** substitutes OE.HID_VAD by OE.HID_TC_VAD_Exp (to support the security objective for the TOE OT.TOE_TC_VAD_Imp)

3) **PP SSCD KG TCSCA** substitutes OE.DTBS_Protect by OE.SCA_TC_DTBS_Exp (to support the security objective for the TOE OT.TOE_TC_DTBS_Imp)

d) The security functional requirements (SFRs) for the TOE include all SFRs of **PP SSCD KG** and in addition:

1) FIA_API.1 (Authentication Proof of Identity) specified in **PP SSCD KG TCCGA**

2) FDP_DAU.2/SVD (Data Authentication with Identity of Guarantor) specified in **PP SSCD KG TCCGA**

3) FTP_ITC.1/SVD (Inter-TSF trusted channel) specified in **PP SSCD KG TCCGA**

4) FDP_UIT.1/DTBS (Data exchange integrity) specified in **PP SSCD KG TCSCA**

5) FTP_ITC.1/VAD (Inter-TSF trusted channel – TC Human Interface Device) specified in **PP SSCD KG TCSCA**

6) FTP_ITC.1/DTBS (Inter-TSF trusted channel – Signature creation Application) specified in **PP SSCD KG TCSCA**

e) **PP SSCD KG TCCGA** provides operation of the SFR FIA_UAU.1 of **PP SSCD KG**.

f) **PP SSCD KG TCSCA** provides refinements for the SFR FIA_UAU.1 of **PP SSCD KG**.

g) The SARs specified in **PP SSCD KG**, **PP SSCD KG TCCGA** and **PP SSCD KG TCSCA** are identical.

5.3.1 PP Claims Rationale

This chapter provides the rationale over the protection profiles **PP SSCD KG**, **PP SSCD KG TCCGA** and **PP SSCD KG TCSCA** which are part of the conformance claim of this ST.

It also describes the additions to the content of the protection profiles **PP SSCD KG**, **PP SSCD KG TCCGA** and **PP SSCD KG TCSCA** for

a) the required use of the PACE authentication method

b) the possibility of generating **mass signatures**[47]

[42] This security objective only applies in case a communication channel to the CGA (via trusted channel) in the Life Cycle Phase “Usage/Operational” is needed.

[43] The TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.

[44] This security objective only applies in case a communication channel to the CGA (via trusted channel) in the Life Cycle Phase “Usage/Operational” is needed.

[45] The TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.

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

[47] Mass signature generation is used to create either a limited or unlimited number of electronic signatures in a row for an automated process.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

Password Authenticated Connection Establishment (PACE) functionality to provide a secure channel for the communication with a legitimate card holder in the Phase “Usage/Operational” has been added. This implies the additions described in the following sub-chapters, which are adapted from the protection profiles [BSI-CC-PP-0056-V2-2012-MA-02], [BSI-CC-PP-0086-2015] and [BSI-CC-PP-0068-V2-2011-MA-01].

5.3.1.1 Security Problem Definition

The Security Problem Definition of the protection profiles are completely taken over and extended by

- three secondary assets
- one subject
- two threats and
- two assumptions

One threat has been extended by an additional note.

Assets, Users and Threat Agents

PACE The following secondary assets taken from [BSI-CC-PP-0068-V2-2011-MA-01] have been added

a) Accessibility to the TOE functions and data only for authorized subjects: property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorized subjects only.

b) TOE internal secret cryptographic keys: permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality. The confidentiality and integrity of the cryptographic keys must be maintained.

c) TOE internal non-secret cryptographic material: permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SOD containing digital signature) used by the TOE in order to enforce its security functionality. The integrity and authenticity of the non-secret cryptographic material must be maintained.

PACE The following subject referring the PACE functionality adapted from [BSI-CC-PP-0068-V2-2011-MA-01] has been added

1. PACE Terminal (CGA and SCA) (corresponding to “Basic Inspection System with PACE” in [BSI-CC-PP-0068-V2-2011-MA-01], which does not exist within the SSCD-context)

PACE The following threats taken from [BSI-CC-PP-0068-V2-2011-MA-01] have been added

T.Skimming (Skimming SSCD / Capturing Card-Terminal Communication)

Adverse action: An attacker imitates a PACE Terminal in order to get access to the user data stored on or transferred between the TOE and the PACE Terminal connected via the contactless/contact interface of the TOE.

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

Asset: confidentiality of VAD

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

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

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

Asset: confidentiality of VAD

The threat T.Hack_Phys (Physical attacks through the TOE interfaces) taken from PP SSCD KG has been extendend by the note:

1. This threat is also directed against the PACE session keys (PACE-KMAC, PACE-KEnc), the ephemeral private key ephem-SKPICC-PACE, Chip Authentication private key, Administrator Personalization Key and Chip Authentication session keys (CA-KMAC, CA-KEnc).

Conclusion:

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

- The assets, subjects and threats in this ST do not change the assets, subjects and threats in the PPs.
- The assets, subjects and threats in this ST are a super set of the assets, subjects and threats in the PPs.
- The assets, subjects and threats in this ST are consistent with the assets, subjects and threats in the PPs.

Assumptions

The following assumptions have been added

A.Env_Admin (Environment for administrator)

TOE initialization, TOE personalization by the Administrator only takes place within a trusted environment. AQES update (generation of SCD/SVD pair, export of SVD and optional creation/update of EFs / DFs) is performed by the Administrator through a trusted channel as a trusted environment.

A.Env_Mass_Signature (Environment for a mass signature TOE)

Mass signature generation only takes place within a trusted environment.

These assumptions do not

1. mitigate a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the PPs because the data, TOE interfaces or signature-creation function which are attacked by
   a) T.SCD_Divulg (Storing, copying and releasing of the signature creation data)
   b) T.SCD_Derive (Derive the signature creation data)
   c) T.Hack_Phys (Physical attacks through the TOE interfaces)
   d) T.SVD_Forgery (Forgery of the signature verification data)
   e) T.SigF_Misuse (Misuse of the signature creation function of the TOE)
   f) T.DTBS_Forgery (Forgery of the DTBS/R)
   g) T.Sig_Forgery (Forgery of the electronic signature)

   are created, stored or configured in the same way whether
   - TOE initialization, TOE personalization by the Administrator takes place within a trusted environment or not,
   - AQES update (generation of SCD/SVD pair, export of SVD and optional creation/update of EFs / DFs) is performed by the Administrator through a trusted channel as a trusted environment or not,
   - Mass signature generation takes place within a trusted environment or not.
2. fulfill an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the PPs because the organizations (and applications used by them), the signature creation system, the requirements for an SSCD laid down in Annex III of the Directive and the usage by the Signatory enforced by the SSCD itself which are described by
   a) P.CSP_QCert (Qualified certificate)
   b) P.QSign (Qualified electronic signatures)
   c) P.Sigy_SSCD (TOE as secure signature creation device)
   d) P.Sig_Non-Repud (Non-repudiation of signatures)

   are not affected, less, modified or the configuration is changed whether
   - TOE initialization, TOE personalization by the Administrator takes place within a trusted environment or not,
   - AQES update (generation of SCD/SVD pair, export of SVD and optional creation/update of EFs / DFs) is performed by the Administrator through a trusted channel as a trusted environment or not,
   - Mass signature generation takes place within a trusted environment or not.

Conclusion:

- The assumptions in this ST do not change the statement made by the assumptions in the PPs.
- The assumptions in this ST are a super set of the assumptions in the PPs.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

- The assumptions in this ST are consistent with the assumptions in the PPs.

5.3.1.2 Security Objectives

The security objectives of the protection profiles are completely taken over and extended by two security objectives for the operational environment. One security objective for the operational environment has been extended by an additional note.

SCA The security objectives taken from **PP SSCD KG TCSCA**:

- OT.TOE_TC_VAD_Imp,
- OT.TOE_TC_DTBS_Imp,
- OE.HID_TC_VAD_Exp and
- OE.SCA_TC_DTBS_Exp

apply only for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.

The security objectives taken from **PP SSCD KG**:

- OE.HID_VAD and
- OE.DTBS_protect

apply for the configuration TC-SCA-CL-Only for contact-based communication.

PACE The security objective OE.Signatory (Security obligation of the signatory) taken from **PP SSCD KG** has been extended by the note:

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

Security Objectives for the Operational Environment

The following security objectives have been added

OE.Env_Admin (Administrator works in trusted environment)

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

OE.Env_Mass_Signature (Mass signatures are generated in trusted environment only)

Mass signature generation only takes place within a trusted environment.

Conclusion:

- The OEs in this ST do not change the statement made by the security objectives in the PPs.
- The security objectives in this ST are a super set of the security objectives in the PPs.
- The security objectives in this ST are consistent with the security objectives in the PPs.

5.3.1.3 Security Requirements

PACE The following security requirements have been added from the protection profiles [BSI-CC-PP-0056-V2-2012-MA-02] and [BSI-CC-PP-0068-V2-2011-MA-01]:

1) FCS_CKM.1/DH_PACE
2) FCS_CKM.1/CA
3) FCS_CKM.4 (the scope of the existing SFR has been extended)
4) FCS_COP.1/PACE_ENC
5) FCS_COP.1/PACE_MAC
6) FCS_COP.1/CA_ENC
7) FCS_COP.1/CA_MAC
8) FDP_ACC.1/TRM

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

9) FDP_ACF.1/TRM
10) FDP_UCT.1/TRM
11) FDP_UIT.1/TRM
12) FIA_UID.1 (the existing SFR has been extended)
13) FIA_UAU.1 (the existing SFR has been extended)
14) FIA_UAU.4/PACE
15) FIA_UAU.5/PACE
16) FIA_UAU.6/PACE
17) FIA_UAU.6/CA
18) FIA_AFL.1/PACE
19) FMT_SMR.1 (the existing SFR has been extended)
20) FMT_MTD.1/KEY_READ
21) FMT_MTD.1/CAPK
22) FPT_EMS.1/KEYS

Additional protection against attacks against the PACE passwords is addressed by

1) FIA_AFL.1/Suspend_PIN
2) FIA_AFL.1/Block_PIN

taken from protection profile [BSI-CC-PP-0086-2015].

The following security requirements have been added to this ST:

1) FCS_CKM.1/RSA (adds generation of a RSA SCD/SVD pair to this ST, iterated)
2) FCS_COP.1/SHA (adds SHA-2 to this ST, not iterated)
3) FCS_COP.1/RSA (adds RSA signature generation to this ST, iterated)
4) FCS_COP.1/AES_MAC (adds AES in CMAC mode for the symmetric authentication mechanism based on AES to this ST, not iterated)
5) FIA_AFL.1/PIN (adds failure handling of PINs other than the signatory PIN to this ST, iterated)
6) FIA_AFL.1/AuthAdmin (adds failure handling of Administrator Personalization Key to this ST, not iterated)
7) FIA_UAU.6/Signature_Creation (adds re-authenticating for signature creation to this ST, not iterated)
8) FCS_RNG.1 (correlates with FCS_RND.1 of [BSI-CC-PP-0068-V2-2011-MA-01]) taken from [BSI-CC-PP-0084-2014]

Some SFRs as defined in **PP SSCD KG** have been renamed to avoid mistakes with the newly added SFRs listed above. These are:

SFR in PP SSCD KG	SFR in this ST
FCS_CKM.1	FCS_CKM.1/EC
FCS_COP.1	FCS_COP.1/EC
FIA_AFL.1	FIA_AFL.1/RAD
FPT_EMS.1	FPT_EMS.1/SSCD

The informative data of SFR "FMT_MTD.1/Admin" after the slash is replaced by "RAD" to FMT_MTD.1/RAD for mnemonic reason because this SFR is refined. In this ST the RAD is created by the Signatory instead of the Administrator.

The following Security requirements have been refined in this ST:

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

1) FDP_ACF.1/SCD/SVD_Generation (After issuing the TOE the administrator is allowed to generate SCD/SVD pair only after successful Chip Authentication Protocol Version 1 following PACE authentication using the PIN.ADMIN as the shared password)
2) FDP_ACF.1/SVD_Transfer (After issuing the TOE the administrator is allowed to export SVD only after successful Chip Authentication Protocol Version 1 PACE authentication using the PIN.ADMIN as the shared password)
3) FDP_ACF.1/Signature_Creation (Signatory is allowed to create electronic signatures only after successful PACE authentication using the PIN.CH or CAN as the shared password and successful authentication against RAD[48])

PACE 4) FDP_RIP.1 (any previous information content of a resource is made unavailable upon the de-allocation of the resource additionally from the objects session keys and the ephemeral private key ephem-SK_{PICC}-PACE)

5) FIA_AFL.1/RAD (security requirement applies to RAD of the signatory PIN)
6) FIA_AFL.1/PIN (security requirement applies to PINs other than the signatory PIN)

PACE 7) FMT_SMR.1 (added the subject PACE Terminal to the roles maintained by the TSF)

8) FMT_MSA.2 (added secure values of the combinations of security attributes)
9) FMT_MTD.1/RAD (the RAD is created by the Signatory once only after successful authentication with the transport PIN)
10) FMT_MTD.1/CAPK (The administrator has the ability to load the Chip Authentication Private Key before issuing the TOE)

These security requirements introduce functionality to this ST which

- is not foreseen in the PP and therefore
- does not affect the functionality as described by the statement of security requirements of the PP.

Conclusion:

- The security requirements added to content of the PPs in this ST do not change the statement of security requirements in the PPs.
- The security requirements in this ST is a super set of the security requirements in the PPs.
- The security requirements in this ST are consistent with the statement of security requirements in the PPs.

[48] Applies only for the configurations TC-SCA-Mandatory for all communication interfaces and TC-SCA-CL-Only in case of contactless communication only.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

6 Security Problem Definition (ASE_SPD)

6.1 Assets, Users and Threat Agents

The Common Criteria define assets as entities that the owner of the TOE presumably places value upon. The term “asset” is used to describe the threats in the operational environment of the TOE.

6.1.1 Assets and objects

a) SCD: private key used to perform an electronic signature operation. The confidentiality, integrity and signatory’s sole control over the use of the SCD shall be maintained.

b) SVD: public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported shall be maintained.

c) DTBS and DTBS/R: set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature shall be maintained.

PACE **Secondary assets taken from [BSI-CC-PP-0068-V2-2011-MA-01]**

d) Accessibility to the TOE functions and data only for authorized subjects: property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorized subjects only.

e) TOE internal secret cryptographic keys: permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality. The confidentiality and integrity of the cryptographic keys must be maintained.

f) TOE internal non-secret cryptographic material: permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SOD containing digital signature) used by the TOE in order to enforce its security functionality. The integrity and authenticity of the non-secret cryptographic material must be maintained.

6.1.2 Users and subjects acting for users

a) User: end user of the TOE who is a human or an IT entity acting on their behalf and 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.

b) Administrator: user who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.

c) 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.

PACE **Subject referring the PACE functionality adapted from [BSI-CC-PP-0068-V2-2011-MA-01]**

a) PACE Terminal (CGA and SCA) (corresponding to “Basic Inspection System with PACE” in **[BSI-CC-PP-0068-V2-2011-MA-01]**, which does not exist within the SSCD-context)

6.1.3 Threat agents

a) 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 a high attack potential and knows no secret.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

6.2 Threats

6.2.1 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.

6.2.2 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.

6.2.3 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.

PACE **Note:**

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

6.2.4 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.

6.2.5 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.

6.2.6 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.

6.2.7 T.Sig_Forgery (Forgery of the electronic signature)

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

PACE

6.2.8 T.Skimming (Skimming SSCD / Capturing Card-Terminal Communication)

Adverse action: An attacker imitates a PACE Terminal in order to get access to the user data stored on or transferred between the TOE and the PACE Terminal connected via the contactless/contact interface of the TOE.

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

Asset: confidentiality of VAD

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Notes:

1. "T.Skimming" has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01]. The term *travel document* has been changed to *SSCD*. The term *an inspection system* has been changed to *a PACE Terminal*. The term *inspecting authority* has been changed to *a PACE Terminal*. The term *logical travel document data* has been changed to a *VAD*.
2. A product using PACE Terminal cannot avert this threat in the context of the security policy defined in PP [BSI-CC-PP-0068-V2-2011-MA-01].
3. Please note that CAN does not effectively represent a secret (but other PACE passwords do so), but is restricted-revealable; i.e. it is either the legitimate user itself or an authorized other person or device (PACE Terminal), cf. OE.Signatory.

PACE

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

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

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

Asset: confidentiality of VAD

Notes:

1. "T.Eavesdropping" has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01]. The term *BIS-PACE* has been changed to *PACE Terminal*. The term *logical travel document data* has been changed to a *VAD*.
2. A product using PACE Terminal cannot avert this threat in the context of the security policy defined in PP [BSI-CC-PP-0068-V2-2011-MA-01].
3. Please note that CAN does not effectively represent a secret (but other PACE passwords do so), but is restricted-revealable; i.e. it is either the legitimate user itself or an authorized other person or device (PACE Terminal), cf. OE.Signatory.

6.3 Organizational Security Policies

6.3.1 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) 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.

6.3.2 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), which is a qualified electronic signature if it is based on a valid qualified certificate (according to **the Directive** Annex I)[49]. 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 an 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.

6.3.3 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**. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

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

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

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

The life cycle 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.

6.4 Assumptions

6.4.1 A.CGA (Trustworthy certification generation application)

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

6.4.2 A.SCA (Trustworthy signature creation application)

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

6.4.3 A.Env_Admin (Environment for administrator)

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

Notes:

1. "A.Env_Admin" is added to the contents of [BSI-CC-PP-0059-2009-MA-02].
2. For initialization and personalization both TOE and Administrator reside in a trusted environment.

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

Notes:

1. The administrator resides in a trusted environment.
2. After authentication and trusted channel establishment communication via trusted channel is considered to be a trusted environment.

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

Mass signature generation only takes place within a trusted environment.

Note:

1. "A.Env_Mass_Signature" is added to the contents of [BSI-CC-PP-0059-2009-MA-02].
2. Trusted Environment means for mass signature generation a physically trusted environment.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

7 Security Objectives (ASE_OBJ)

7.1 Security Objectives for the TOE

7.1.1 Relation between the Claimed PPs

For relation between **PP SSCD KG**, **PP SSCD KG TCCGA** and **PP SSCD KG TCSCA** see section 5.3 Conformance Rationale.

7.1.2 OT.Lifecycle_Security (Life cycle security)

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

Note:

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

7.1.3 OT.SCD/SVD_Auth_Gen (Authorized SCD/SVD generation)

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

7.1.4 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 can practically occur only once and cannot be reconstructed from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligible.

7.1.5 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 a digital signature creation with the SCD.

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

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

Note:

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

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

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

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

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

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

7.1.9 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.

7.1.10 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.

7.1.11 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.

7.1.12 OT.Tamper_Resistance (Tamper resistance)

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

CGA

7.1.13 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.

Note:

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

CGA

7.1.14 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.

Note:

1. This security objective only applies for the Life Cycle Phase “Usage/Operational” as the TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

SCA

7.1.15 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.

Notes:

1. This security objective for the TOE is partly covering OE.HID_VAD from the core **PP SSCD KG**. While OE.HID_VAD in **PP SSCD KG** requires only the operational environment to protect VAD, **PP SSCD KG TCSCA** 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 **PP SSCD KG TCSCA** 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.
2. This security objective only applies for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.

SCA

7.1.16 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 shall not generate electronic signatures with the SCD for altered DTBS.

Notes:

1. This security objective for the TOE is partly covering OE.DTBS_Protect from the core **PP SSCD KG**. While OE.DTBS_Protect in **PP SSCD KG** requires only the operational environment to protect DTBS, **PP SSCD KG TCSCA** 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 **PP SSCD KG TCSCA** 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.
2. This security objective only applies for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.

7.2 Security Objectives for the Operational Environment

7.2.1 Relation between the Claimed PPs

For relation between **PP SSCD KG**, **PP SSCD KG TCCGA** and **PP SSCD KG TCSCA** see section 5.3 Conformance Rationale.

7.2.2 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.

7.2.3 OE.CGA_QCert (Generation of qualified certificates)

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

a) the name of the signatory controlling the TOE;

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

c) the advanced signature of the CSP.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

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

7.2.4 OE.HID_VAD (Protection of the VAD)

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

Note:

1. This security objective applies particularly for the configuration **TC-SCA-CL-Only** in case of contact-based communication, where the TOE does not require a trusted channel for import of the VAD.

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

The signatory shall use a trustworthy SCA that:

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

Note:

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

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

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

Note:

1. This security objective applies particularly for the configuration **TC-SCA-CL-Only** in case of contact-based communication, where the TOE does not require a trusted channel for import of the DTBS/R.

7.2.7 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.

Note:

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

CGA

7.2.8 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, personalizes the TOE for the legitimate user as signatory, links the identity of the TOE as SSCD with the identity of the legitimate user, and delivers the TOE to the signatory.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Notes:

1. This objective replaces OE.SSCD_Prov_Service from the core **PP SSCD KG**, which is possible as it does not imply any additional requirements for the operational environment when compared to OE.SSCD_Prov_Service (OE.Dev_Prov_Service is a subset of OE.SSCD_Prov_Service).
2. The preparation of the TOE for proof as SSCD to external entities only applies in case a communication channel to the CGA (via trusted channel) in the Life Cycle Phase “Usage/Operational” is needed.

CGA

7.2.9 OE.CGA_SSCD_Auth (Pre-initialization 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.

Note:

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

CGA

7.2.10 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.

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

Note:

1. This security objective only applies for the Life Cycle Phase “Usage/Operational” as the TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.

SCA

7.2.11 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.

Notes:

1. This security objective for the TOE is partly covering OE.HID_VAD from the core **PP SSCD KG**. While OE.HID_VAD in **PP SSCD KG** requires only the operational environment to protect VAD, **PP SSCD KG TCSCA** 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 **PP SSCD KG TCSCA** 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.
2. This security objective only applies for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

SCA

7.2.12 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.

Notes:

1. This security objective for the TOE is partly covering OE.DTBS_Protect from the core **PP SSCD KG**. While OE.DTBS_Protect in **PP SSCD KG** requires only the operational environment to protect DTBS, **PP SSCD KG TCSCA** 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 **PP SSCD KG TCSCA** 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.
2. This security objective only applies for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.

7.2.13 OE.Env_Admin (Administrator works in trusted environment)

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

Notes:

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

7.2.14 OE.Env_Mass_Signature (Mass signatures are generated in trusted environment only)

Mass signature generation only takes place within a trusted environment.

Note:

1. “OE.Env_Mass_Signature” is added to the contents of [BSI-CC-PP-0059-2009-MA-02].

7.3 Security Objective Rationale

7.3.1 Security Objectives Backtracking

The following tables show how the security objectives for the TOE (Table 7-1) and the security objectives for the operational environment (Table 7-2) cover the threats, organizational security policies and assumptions.

Security objectives that are added by **PP SSCD KG TCCGA** or **PP SSCD KG TCSCA** are color coded for better readability.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
T.SCD_Divulg					x										
T.SCD_Derive		x				x									
T.Hack_Phys					x				x	x	x				
T.SVD_Forgery				x									x		
T.SigF_Misuse	x						x	x						x	x
T.DTBS_Forgery								x							x
T.Sig_Forgery			x			x									
PACE T.Skimming														x	
PACE T.Eavesdropping														x	
P.CSP_Qcert	x			x								x			
P.Qsign						x	x								
P.Sigy_SSCD	x	x	x		x	x	x	x	x		x	x	x		
P.Sig_Non-Repud	x		x	x	x	x	x	x	x	x	x	x	x	x	x

Table 7-1: Mapping of security problem definition to security objectives of the TOE (assumptions are mapped in Table 7-2)

	OE.CGA_QCert	OE.SVD_Auth	OE.Dev_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory	OE.Env_Admin	OE.Env_Mass_Signature[50]	OE.CGA_SSCD_Auth	OE.CGA_TC_SVD_Imp	OE.HID_TC_VAD_Exp	OE.SCA_TC_DTBS_Exp
T.SCD_Divulg													
T.SCD_Derive													
T.Hack_Phys													
T.SVD_Forgery		x									x		
T.SigF_Misuse				x	x	x	x					x	x
T.DTBS_Forgery					x	x							x
T.Sig_Forgery	x												
PACE T.Skimming							x						
PACE T.Eavesdropping													
P.CSP_Qcert	x									x			
P.Qsign	x				x								
P.Sigy_SSCD			x							x	x		
P.Sig_Non-Repud	x	x	x		x	x	x			x	x	x	x
A.CGA	x	x											
A.SCA					x								
A.Env_Admin								x					
A.Env_Mass_Signature[51]									x				

Table 7-2: Mapping of security problem definition to security objectives of the operational environment

[50] **Note:** "OE.Env_Mass_Signature" is added to the contents of [BSI-CC-PP-0059-2009-MA-02].

[51] **Note:** "A.Env_Mass_Signature" is added to the contents of [BSI-CC-PP-0059-2009-MA-02].

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

7.3.2 Security Objectives Sufficiency

The rationale for T.SCD_Divulg, T.SCD_Derive, T.Hack_Phys, T.Sig_Forgery and P.QSign remains unchanged as given in **PP SSCD KG**.

The rationale for T.SVD_Forgery, P.CSP_QCert and P.Sigy_SSCD remains unchanged as given in **PP SSCD KG TCCGA**.

The rationale for P.Sig_Non-Repud is a combination of **PP SSCD KG, PP SSCD KG TCCGA** and **PP SSCD KG TCSCA**. The parts relevant to **PP SSCD KG TCCGA** are marginalized with CGA. The parts relevant for **PP SSCD KG TCSCA** are marginalized with **SCA** and apply only for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only. The parts of **PP SSCD KG** that are replaced by the parts relevant for **PP SSCD KG TCSCA** still apply for the configuration TC-SCA-CL-Only for contact-based communication.

The rationale for T.SigF_Misuse and T.DTBS_Forgery is a combination of **PP SSCD KG** and **PP SSCD KG TCSCA**. The parts relevant for **PP SSCD KG TCSCA** are marginalized with **SCA** and apply only for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only. The parts of **PP SSCD KG** that are replaced by the parts relevant for **PP SSCD KG TCSCA** still apply for the configuration TC-SCA-CL-Only for contact-based communication.

The rationale how security objectives address the assumptions A.Env_Admin *(Environment of Administrator)* and A.Env_Mass_Signature *(Environment for a mass signature TOE)* has been added.

Countering of threats by security objectives:

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

- OT.SCD_Secrecy, which assures the secrecy of the SCD used for signature creation.

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

- OT.SCD/SVD_Auth_Gen counters this threat by implementing cryptographically secure generation of the SCD/SVD pair.
- OT.Sig_Secure ensures cryptographically secure electronic signatures.

T.Hack_Phys (*Exploitation of physical vulnerabilities*) 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.

CGA **T.SVD_Forgery** (*Forgery of the signature verification data*) deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate[52]. 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 and verification of the correspondence between the SCD in the SSCD of the signatory and the SVD in the input it provides to the certificate generation function of the CSP.

Additionally T.SVD_Forgery is addressed by

[52] The TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

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

- OT.Lifecycle_Security (*Lifecycle security*) requires the TOE to detect flaws during the initialization, personalization and operational usage including secure destruction of the SCD, which may be initiated by the signatory.
- OT.Sigy_SigF (*Signature creation function for the legitimate signatory only*) ensures that the TOE provides the signature creation function for the legitimate signatory only.
- OE.DTBS_Intend (*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.

SCA **For the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only (as given in PP SSCD KG TCSCA):**

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

- OE.HID_TC_VAD_Exp (*Trusted channel of HID for VAD*) and
- OT.TOE_TC_VAD_Imp (*Trusted channel of TOE for VAD*).

For the configuration TC-SCA-CL-Only in case of contact-based communication (as given in PP SSCD KG):

- OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between SCA and the TOE.
- OE.HID_VAD (Protection of the VAD) provides confidentiality and integrity of the VAD as needed by the authentication method employed.

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

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

- OE.DTBS_Intend, 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.

SCA **For the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only (as given in PP SSCD KG TCSCA):**

The threat T.DTBS_Forgery is addressed by the security objectives

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

- 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.

For the configuration TC-SCA-CL-Only in case of contact-based communication (as given in PP SSCD KG):

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

- OE.DTBS_Protect, which ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE.

T.Sig_Forgery (*Forgery of the electronic signature*) 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 and ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance.
- OE.CGA_QCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

PACE **T.Skimming** addresses accessing the VAD (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless/contact interface. This threat is countered by the security objective

- OT.TOE_TC_VAD_Imp through the PACE authentication.

The objective

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

PACE **T.Eavesdropping** addresses listening to the communication between the TOE and a rightful terminal in order to gain the VAD transferred there. This threat is countered by the security objective

- OT.TOE_TC_VAD_Imp through a trusted channel based on the PACE authentication.

Enforcement of OSPs by security objectives:

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

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

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[53].
- The OE.CGA_SSCD_Auth ensures that the SP checks the proof of the device presented of the applicant that it is a SSCD[54].

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

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

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

- The OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE to the CGA corresponds to the SCD stored in the TOE and used by the signatory.
- The OT.Lifecycle_Security ensures that the TOE detects flaws during the initialization, personalization and operational usage.

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

- 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.

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

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

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

- OT.Lifecycle_Security,
- OT.SCD/SVD_Gen and
- OT.Sigy_SigF.

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

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

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

- OE.Dev_Prov_Service ensures that the signatory uses an authentic TOE, initialized and personalized for the signatory.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

- 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).

CGA **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.

- 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.

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.

- 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.

SCA **For the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only (as given in PP SSCD KG TCSCA):**

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.

For the configuration TC-SCA-CL-Only in case of contact-based communication (as given in PP SSCD KG):

- OE.DTBS_Intend,
- OE.DTBS_Protect 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.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Upkeep of assumptions by security objectives:

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

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

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

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

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

Notes:

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

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

Note:

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

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

8 Extended Components Definition (ASE_ECD)

This Security Target uses the following extended components:

- **FPT_EMS** as defined in [BSI-CC-PP-0059-2009-MA-02]
- **FIA_API** as defined in [BSI-CC-PP-0071-2012-MA-01]
- **FCS_RNG** as defined in [BSI-CC-PP-0084-2014]

No other components are used.

8.1 Definition of the Family FCS_RNG

To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

FCS_RNG Generation of random numbers

Family behavior

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

Component levelling:

FCS_RNG Generation of random numbers	1

FCS_RNG.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RNG.1 There are no management activities foreseen.
Audit:	FCS_RNG.1 There are no actions defined to be auditable.

FCS_RNG.1	**Random number generation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].
FCS_RNG.1.2	The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

Note:

1. A physical random number generator (RNG) produces the random number by a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes, mouse movement). A deterministic RNG uses a random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs where a hybrid physical RNG produces at least the amount of entropy the RNG output may contain and the internal state of a hybrid deterministic RNG output contains fresh entropy but less than the output of RNG may contain.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

9 Security Requirements (ASE_REQ)

9.1 Security Functional Requirements

9.1.1 Use of Requirement Specifications

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

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

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

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

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

9.1.2 Cryptographic Support (FCS)

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

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/EC	The TSF shall generate an SCD/SVD pair in accordance with a specified cryptographic key generation algorithm **Elliptic Curve EC Key Generation**[55] and specified cryptographic key sizes **see below**[56] that meet the following:

ECDSA Key Generation:

1. **According to the appendix A4.3 in [ANSI-X9.62] the cofactor h is not supported.**
2. **According to section 6.4.2 in [ISO-IEC-14888-3]**
3. **According to appendix A.16.9 in [IEEE-1363]**

using curves

1. **for key size 256 bits:**
   a) **P-256 ([NIST-FIPS-186-4], chapter D.2.3 "Curve P-256", aka secp256r1)**
   b) **brainpoolP256r1 ([RFC-5639-2010-03], chapter 3.4)**
2. **for key size 384 bits:**
   a) **P-384 ([NIST-FIPS-186-4], chapter D.2.4 "Curve P-384", aka secp384r1)**
   b) **brainpoolP384r1 ([RFC-5639-2010-03], chapter 3.6)**
3. **for key size 512 bits:**

[55] [assignment: cryptographic key generation algorithm]

[56] [assignment: cryptographic key sizes]

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

brainpoolP512r1 ([RFC-5639-2010-03], chapter 3.7)

4. **for key size 521 bits:**

P-256 ([NIST-FIPS-186-4], chapter D.2.5 "Curve P-521", aka secp521r1)[57]

Notes:

1. FCS_CKM.1/EC amounts to requirement "FCS_CKM.1" with the selection of ECC key generation.
2. This TOE uses the crypto libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010 of the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12).
3. For the cryptographic key generation algorithm "Elliptic Curve EC Key Generation" see [Infineon-ST-M7892-D11-G12], 7.1.4.8 Elliptic Curve (EC) key generation.
4. If a configuration of the TOE uses FCS_CKM.1/RSA, it must not use this SFR additionally.

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

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/RSA	The TSF shall generate an SCD/SVD pair in accordance with a specified cryptographic key generation algorithm **RSA Key Generation**[58] and specified cryptographic key sizes **2048 or 3072 bits**[59] that meet the following: 1. **According to section 3.1 and 3.2 in [RSA-PKCS1-v2.2]: for u=2, i.e., without any (r_i, d_i, t_i), i > 2, 3.1 supported for n < $2^{3072 + 128}$, 3.2(1) supported for n< $2^{2048 + 64}$, 3.2(2) supported for p x q < $2^{3072 + 128}$** 2. **According to section 8.1.3.1 in [IEEE-1363]: 8.1.3.1(1) supported for n < $2^{2048 + 64}$, 8.1.3.1(2) supported for p x q < $2^{3072 + 128}$, 8.1.3.1(3) supported for p x q < $2^{2048 + 64}$.**[60]

Notes:

1. FCS_CKM.1/RSA is added to contents of PP [BSI-CC-PP-0059-2009-MA-02] (iterated).
2. This TOE uses the crypto libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010 of the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12).
3. For the cryptographic key generation algorithm "RSA Key Generation" see [Infineon-ST-M7892-D11-G12] 7.1.4.5 Rivest-Shamir-Adleman (RSA) key generation.
4. The standard PKCS #1 version 2.2 [RSA-PKCS1-v2.2] supersedes the standard PKCS #1 version 2.1, which is referenced in the [Infineon-ST-M7892-D11-G12]. However, version 2.2 only includes compatible techniques; both versions are equivalent in this context.
5. If a configuration of the TOE uses FCS_CKM.1/EC, it must not use this SFR additionally.

PACE

9.1.2.3 FCS_CKM.1/DH_PACE (Cryptographic key generation – Diffie-Hellman for PACE session keys)

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]

[57] [assignment: list of standards]

[58] [assignment: cryptographic key generation algorithm]

[59] [assignment: cryptographic key sizes]

[60] [assignment: list of standards]

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Justification: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/DH_PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH compliant to [BSI-TR-03111-V200-ECC]**[61] and specified cryptographic key sizes **192, 256 bits (for AES)**[62] that meet the following:

[ICAO-TR-110]

using curves

see section 9.1.2.1 FCS_CKM.1/EC (Cryptographic key generation – EC)[63]**.**

Notes:

1. This SFR has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01].
2. See also FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC for the key sizes used.
3. The TOE generates a shared secret value K with the terminal during the PACE protocol, see [ICAO-TR-110]. The shared secret value K is used for deriving the AES session keys for message encryption and message authentication (PACE-K.MAC, PACE-K.Enc) according to [ICAO-TR-110] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.
4. FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [ICAO-TR-110].
5. See also Appendix A: Overview Cryptographic Algorithms, Cryptographic Primitive No. 15 for SHA-2.
6. The TOE destroys any session keys in accordance with FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011-MA-01] after
   i. detection of an error in a received command by verification of the MAC and
   ii. The TOE clears the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.

CA

9.1.2.4 FCS_CKM.1/CA (Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys)

Hierarchical to: No other components.

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

FCS_CKM.1.1/CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH**[64] and specified cryptographic key sizes **192, 256 bits (for AES)**[65] that meet the following:

based on an ECDH protocol compliant to [BSI-TR-03111-V200-ECC]

using curves

see section 9.1.2.1 FCS_CKM.1/EC (Cryptographic key generation – EC)[66]**.**

Notes:

1. This SFR has been adapted from [BSI-CC-PP-0056-V2-2012-MA-02].
2. See also FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the key sizes used.

[61] [assignment: cryptographic key generation algorithm]

[62] [assignment: cryptographic key sizes]

[63] [assignment: list of standards]

[64] [assignment: cryptographic key generation algorithm]

[65] [assignment: cryptographic key sizes]

[66] [assignment: list of standards]

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

3. The TOE generates a shared secret value K with the terminal during the Chip Authentication Protocol Version 1, see [BSI-TR-03110-1-V220]. The protocol used by this TOE bases on the Diffie-Hellman-Protocol compliant to [BSI-TR-03111-V200-ECC] (i.e. an elliptic curve cryptography algorithm) (cf. [BSI-TR-03111-V200-ECC], for details). The shared secret value is used to derive the Chip Authentication Session Keys (CA-K.MAC, CA-K.Enc) used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [BSI-TR-03110-1-V220]).
4. The TOE implements the hash function SHA-256 for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms according to [BSI-TR-03111-V200-ECC].
5. See also Appendix A: Overview Cryptographic Algorithms, Cryptographic Primitive No. 15 for SHA-2.
6. The TOE destroys any session keys in accordance with FCS_CKM.4 from [BSI-CC-PP-0068-V2-2011-MA-01] after
   i. detection of an error in a received command by verification of the MAC and
   ii. after successful run of the Chip Authentication Protocol Version 1.
   iii. The TOE destroys the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys.
   iv. The TOE clears the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.

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

9.1.2.5 FCS_CKM.4 (Cryptographic key destruction)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting the key with zeros**[67] that meet the following: **none**[68]**.**

Notes:

1. The cryptographic key SCD will be destroyed on demand of the signatory. The signatory may want to destruct the SCD stored in the SSCD e.g. after the qualified certificate for the corresponding SVD is not valid anymore.

PACE 2. The TOE shall destroy the PACE session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/EC	The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm **Elliptic Curve Digital Signature Algorithm (ECDSA)**[69] and cryptographic key sizes **256, 384, 512 or 521 bits**[70] that meet the following: **Signature Generation:** **1. According to section 7.3 in [ANSI-X9.62]. Not implemented is step d) and e) thereof. The output of step e) has to be provided as input to our function by the caller. Deviation of step c) and f): The jumps to step a)**

[67] [assignment: cryptographic key destruction method]

[68] [assignment: list of standards]

[69] [assignment: cryptographic algorithm]

[70] [assignment: cryptographic key sizes]

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

were substituted by a return of the function with an error code, the jumps are emulated by another call to our function.

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

using curves

see section 9.1.2.1 FCS_COP.1/EC (Cryptographic operation – EC)[71].

Notes:

1. FCS_COP.1/EC amounts to requirement "FCS_COP.1" with the selection of ECDSA.
2. This TOE uses the crypto libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010 of the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12).
3. For the "Elliptic Curve Digital Signature Algorithm (ECDSA)" see [Infineon-ST-M7892-D11-G12], 7.1.4.7 Elliptic Curve DSA (ECDSA) Signature Generation and Verification.
4. If a configuration of the TOE uses FCS_COP.1/RSA, it must not use this SFR additionally.

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/RSA	The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm **Rivest-Shamir-Adleman (RSA)[72]** and cryptographic key sizes **2048 or 3072 bits[73]** that meet the following:

Signature Generation (with or without CRT):

1. **According to section 5.2.1 RSASP1 in** [RSA-PKCS1-v2.2]**: for u=2, i.e., without any (r_i, d_i, t_i), i > 2 – 5.2.1(1) not supported, 5.2.1(2.a) supported for n <$2^{2048 + 64}$, 5.2.1(2b) supported for p x q < $2^{3072 + 128}$, 5.2.1(2b) (ii)&(v) not applicable due to u = 2**
2. **According to section 8.2.4 in [IEEE-1363]: 8.2.1(I) supported for n < $2^{2048 + 64}$, 8.2.1(II) supported for p x q < $2^{3072 + 128}$, 8.2.1(III) not supported[74].**

Notes:

1. FCS_COP.1/RSA is added to contents of PP [BSI-CC-PP-0059-2009-MA-02] (iterated).
2. This TOE uses the crypto libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010 of the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12).
3. For the "Rivest-Shamir-Adleman (RSA)" see [Infineon-ST-M7892-D11-G12], 7.1.4.4 Rivest-Shamir-Adleman (RSA) operation.
4. The standard PKCS #1 version 2.2 [RSA-PKCS1-v2.2] supersedes the standard PKCS #1 version 2.1, which is referenced in the [Infineon-ST-M7892-D11-G12]. However, version 2.2 only includes compatible techniques; both versions are equivalent in this context.
5. The padding is done according to RSASSA-PSS and RSASSA-PKCS1-v1_5.
6. If a configuration of the TOE uses FCS_COP.1/EC, it must not use this SFR additionally.

[71] [assignment: list of standards]

[72] [assignment: cryptographic algorithm]

[73] [assignment: cryptographic key sizes]

[74] [assignment: list of standards]

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] not fulfilled, but **justified**: A hash function does not use any cryptographic key; hence, neither a respective key import nor key generation can be expected here. FCS_CKM.4 Cryptographic key destruction not fulfilled, but **justified**: A hash function does not use any cryptographic key; hence, a respective key destruction cannot be expected here.
FCS_COP.1.1/SHA	The TSF shall perform **hash-value calculation of user chosen data**[75] in accordance with a specified cryptographic algorithm **SHA-224, SHA-256, SHA-384 and SHA-512**[76] and cryptographic key sizes **none**[77] that meet the following: **[NIST-FIPS-180-4] with chapters 6.2 "SHA-256", 6.3 "SHA-224", 6.4 "SHA-512" and 6.5 "SHA-384"**[78]**.**

Notes:

1. FCS_COP.1/SHA is added to contents of PP [BSI-CC-PP-0059-2009-MA-02] (not iterated).
2. This TOE uses the crypto libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010 of the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12).

PACE

3. The requirements for the hashing functions used for PACE are included in SFR FCS_CKM.1/DH_PACE.
4. FCS_COP.1/SHA is used for internally calculated hash values which are used afterward for the signature creation including last round hash values.
5. For the "hash-value calculation of user chosen data" in case of SHA-256 and SHA-512 see [Infineon-ST-M7892-D11-G12], 7.1.4.10 SHA-2 Operation.
6. A SHA-224 value is computed by CardOS DI V5.4 from a SHA-256 value according to [NIST-FIPS-PUB-180-4] chapter 6.3.
7. A SHA-384 value is computed by CardOS DI V5.4 from a SHA-512 value according to [NIST-FIPS-PUB-180-4] chapter 6.5.

PACE

9.1.2.9 FCS_COP.1/PACE_ENC (Cryptographic operation – Encryption / Decryption AES)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: **fulfilled by FCS_CKM.1/DH_PACE** FCS_CKM.4 Cryptographic key destruction: **fulfilled by FCS_CKM.4**
FCS_COP.1.1/PACE_ENC	The TSF shall perform **secure messaging - encryption and decryption**[79] in accordance with a specified cryptographic algorithm **AES in CBC mode**[80] and cryptographic key sizes **192, 256 bit**[81] that meet the following: **compliant to [ICAO-TR-110]**[82].

[75] [assignment: list of cryptographic operations]

[76] [assignment: cryptographic algorithm]

[77] [assignment: cryptographic key sizes]

[78] [assignment: list of standards]

[79] [assignment: list of cryptographic operations]

[80] [assignment: cryptographic algorithm]

[81] [assignment: cryptographic key sizes]

[82] [assignment: list of standards]

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Notes:

1. This SFR has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01].
2. This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K.Enc).

PACE

9.1.2.10 FCS_COP.1/PACE_MAC (Cryptographic operation – MAC)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_COP.1.1/PACE_MAC	The TSF shall perform **secure messaging – message authentication code generation and verification**[83] in accordance with a specified cryptographic algorithm **AES in CMAC mode**[84] and cryptographic key sizes **192, 256 bit**[85] that meet the following: **compliant to [ICAO-TR-110]** [86].

Notes:

1. This SFR has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01].
2. This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K.Mac).

CA

9.1.2.11 FCS_COP.1/CA_ENC (Cryptographic operation – Symmetric Encryption / Decryption AES)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/CA_ENC	The TSF shall perform **secure messaging - encryption and decryption**[87] in accordance with a specified cryptographic algorithm **AES in CBC mode**[88] and cryptographic key sizes **192, 256 bit**[89] that meet the following: **[NIST-FIPS-197] and [NIST-800-38A-2001]**[90].

Notes:

1. This SFR has been adapted from [BSI-CC-PP-0056-V2-2012-MA-02].
2. This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication protocol according to the FCS_CKM.1/CA.

CA

9.1.2.12 FCS_COP.1/CA_MAC (Cryptographic operation – MAC)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or

[83] [assignment: list of cryptographic operations]

[84] [assignment: cryptographic algorithm]

[85] [assignment: cryptographic key sizes]

[86] [assignment: list of standards]

[87] [assignment: list of cryptographic operations]

[88] [assignment: cryptographic algorithm]

[89] [assignment: cryptographic key sizes]

[90] [assignment: list of standards]

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

	FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/CA_MAC	The TSF shall perform **secure messaging – message authentication code**[91] in accordance with a specified cryptographic algorithm **AES in CMAC mode**[92] and cryptographic key sizes **192, 256 bit**[93] that meet the following: **[NIST-FIPS-197] and [ISO-IEC-9797-1-2011]**[94].

Notes:

1. This SFR has been adapted from [BSI-CC-PP-0056-V2-2012-MA-02].
2. This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA.

CA

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] not fulfilled, but **justified**: The key used here is imported by the administrator and made unavailable at the end of the TOE preparation. FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AES_MAC	The TSF shall perform **message authentication code in CMAC**[95] in accordance with a specified cryptographic algorithm **Advanced Encryption Standard (AES) in CMAC mode**[96] and cryptographic key sizes **128, 192, 256 bit**[97] that meet the following: **[NIST-FIPS-197] and [ISO-IEC-9797-1-2011]**[98].

Notes:

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

PACE

9.1.2.14 FCS_RNG.1 (Random number generation)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a **hybrid deterministic**[99] random number generator that implements:
(DRG.4.1)	**The internal state of the RNG shall use PTRNG of class PTG.2 as random source.**
(DRG.4.2)	**The RNG provides forward secrecy.**
(DRG.4.3)	**The RNG provides backward secrecy even if the current internal state is known.**
(DRG.4.4)	**The RNG provides enhanced forward secrecy for every call.**

[91] [assignment: list of cryptographic operations]

[92] [assignment: cryptographic algorithm]

[93] [assignment: cryptographic key sizes]

[94] [assignment: list of standards]

[95] [assignment: list of cryptographic operations]

[96] [assignment: cryptographic algorithm]

[97] [assignment: cryptographic key sizes]

[98] [assignment: list of standards]

[99] [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

(DRG.4.5) The internal state of the RNG is seeded by a PTRNG of class PTG.2 according to [BSI-AIS31-V3]. [100]

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

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

(DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A as defined in [BSI-AIS20-V2]. [101]

Notes:

1. This SFR has been adapted from [BSI-CC-PP-0084-2014] (FCS_RNG.1) to meet [BSI-AIS20-V2]. It correlates with the SFR 'FCS_RND.1' from [BSI-CC-PP-0068-V2-2011-MA-01].
2. This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocol (PACE) as required by FIA_UAU.4/PACE.
3. Entropy source uses PTG.2 of the hardware as noise source and Block_Cipher_df as specified in SP800-90A using the AES block cipher as a conditioning component.
4. [NIST-SP800-90A] C.3: each generate request may produce no more than 2^{19} bits, which means 2^{12} 128-bit blocks. In an ideal random sequence of 2^{12} 128-bit blocks, the probability that any two blocks will be the same is approximately 2^{-105}.

9.1.3 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	authorized, not authorized
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)

Table 9-1: Subjects and security attributes for access control

PACE

9.1.3.1 FDP_ACC.1/TRM (Subset access control – Terminal Access)

Hierarchical to: No other components.

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

FDP_ACC.1.1/TRM The TSF shall enforce the **Access_Control_SFP**[102] on **terminals gaining access to the User Data stored in the TOE**[103].

Note:

1. This SFR has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01]. The term *travel document* has been changed to *TOE*.

[100] [assignment: list of security capabilities]

[101] [assignment: a defined quality metric]

[102] [assignment: access control SFP]

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

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

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

PACE

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control: **fulfilled by FDP_ACC.1/TRM** FMT_MSA.3 Static attribute initialization: **not fulfilled, but justified** **The access control TSF according to FDP_ACF.1/TRM uses security attributes having been defined during the personalization and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.**
FDP_ACF.1.1/TRM	The TSF shall enforce the **Access_Control_SFP** to objects based on the following: **1. Subjects:** **a. Terminal** **b. PACE Terminal;** **2. Objects:** **a. data in EF.CardSecurity;** **3. Security attributes:** a. **Authentication status of terminals.**[104]
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: 1. **A PACE Terminal is allowed to read data in EF.CardSecurity according to [ICAO-TR-110] after a successful PACE authentication as required by FIA_UAU.1.**[105]
FDP_ACF.1.3/TRM	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**[106]
FDP_ACF.1.4/TRM	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **1. Any terminal being not authenticated as PACE authenticated PACE Terminal is not allowed to read, to write, to modify, to use any User Data stored on the TOE.** 2. **Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the TOE.**[107]

Notes:

1. This SFR has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01]. The term *travel document* has been changed to *TOE, BIS-PACE* has been changed to *PACE Terminal*.
2. EF.CardSecurity holds the public key needed for authenticating the SSCD during Chip Authentication Protocol Version 1.

9.1.3.3 FDP_ACC.1/SCD/SVD_Generation (Subset access control)

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ SCD/SVD_Generation	The TSF shall enforce the SCD/SVD_Generation_SFP on: 1. subjects: S.User, 2. objects: SCD, SVD,

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

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

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

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

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

3. operations: generation of SCD/SVD pair.

9.1.3.4 FDP_ACF.1/SCD/SVD_Generation (Security attribute based access control)

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1/ SCD/SVD_Generation	The TSF shall enforce the SCD/SVD_Generation_SFP 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 “authorized” is allowed to generate SCD/SVD pair. **After issuing the TOE S.User is allowed to generate SCD/SVD pair only after successful Chip Authentication Protocol Version 1 following PACE authentication using the PIN.ADMIN as the shared password[108].**
FDP_ACF.1.3/ SCD/SVD_Generation	The TSF shall explicitly authorize 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 authorized” is not allowed to generate SCD/SVD pair.

Notes:

1. The changes represent the need to secure communication between the SSCD Issuing Application and the TOE via trusted channel when generating SCD/SVD pair after issuing the TOE.
2. After the TOE is issued the TOE is in phase OPERATIONAL.

9.1.3.5 FDP_ACC.1/SVD_Transfer (Subset access control)

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ SVD_Transfer	The TSF shall enforce the SVD_Transfer_SFP on: 1. subjects: S.User, 2. objects: SVD, 3. operations: export.

9.1.3.6 FDP_ACF.1/SVD_Transfer (Subset access control)

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1/ SVD_Transfer	The TSF shall enforce the SVD_Transfer_SFP to objects based on the following: 1. the S.User is associated with the security attribute Role; **2.** the SVD.
FDP_ACF.1.2/	The TSF shall enforce the following rules to determine if an operation among controlled

[108] is a [REFINEMENT]

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

SVD_Transfer	subjects and controlled objects is allowed: R.Admin[109] is allowed to export SVD. **After issuing the TOE R.Admin is allowed to export SVD only after successful Chip Authentication Protocol Version 1 following PACE authentication using the PIN.ADMIN as the shared password.[110]**
FDP_ACF.1.3/ SVD_Transfer	The TSF shall explicitly authorize 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.

Note:

1. The changes represent the need to secure communication between the CGA and the TOE via trusted channel when exporting the SVD in Life Cycle Phase “Usage/Operational”.

9.1.3.7 FDP_ACC.1/Signature_Creation (Subset access control)

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ Signature_Creation	The TSF shall enforce the Signature_Creation_SFP on: 1. subjects: S.User, 2. objects: DTBS/R, SCD, 3. operations: signature creation.

9.1.3.8 FDP_ACF.1/Signature_Creation (Security attribute based access control)

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1/ Signature_Creation	The TSF shall enforce the Signature_Creation_SFP to objects based on the following: 1. the user S.User is associated with the security attribute “Role”; and 2. the SCD with the security attribute “SCD Operational”
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”. **For the configurations TC-SCA-Mandatory for all communication interfaces and TC-SCA-CL-Only in case of contactless communication: R.Sigy is only allowed to create electronic signatures for DTBS/R with SCD only after successful PACE authentication using the PIN.CH or CAN as the shared password and successful authentication against RAD[111].**
FDP_ACF.1.3/ Signature_Creation	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none
FDP_ACF.1.4/	The TSF shall explicitly deny access of subjects to objects based on the following

[109] [selection: R.Admin, R.Sigy]

[110] is a [REFINEMENT]

[111] is a [REFINEMENT]

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Signature_Creation	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”.

Note:

1. The changes represent the need to secure communication between the SCA and the TOE via trusted channel for all communication interfaces for the configuration **TC-SCA-Mandatory** and only for contactless communication for the configuration **TC-SCA-CL-Only** when creating electronic signatures for DTBS/R with SCD.

PACE

9.1.3.9 FDP_UCT.1/TRM (Basic data exchange confidentiality – Terminal)

Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/TRM
FDP_UCT.1.1/TRM	The TSF shall enforce the **Access_Control_SFP**[112] to be able to **transmit and receive**[113] user data in manner protected from unauthorized disclosure.

Note:

1. This SFR has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01].

PACE

9.1.3.10 FDP_UIT.1/TRM (Data exchange integrity – Terminal)

Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/TRM
FDP_UIT.1.1/TRM	The TSF shall enforce the **Access_Control_SFP**[114] to be able to **transmit and receive**[115] user data in a manner protected from **modification, deletion, insertion and replay**[116] errors.
FDP_UIT.1.2/TRM	The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay**[117] has occurred.

Note:

1. This SFR has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01].

SCA

9.1.3.11 FDP_UIT.1/DTBS (Data exchange integrity – DTBS)

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
FDP_UIT.1.1/DTBS	The TSF shall enforce the Signature_Creation_SFP to receive user data in a manner protected from modification and insertion errors.

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

[113] [selection: transmit, receive]

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

[115] [selection: transmit, receive]

[116] [selection: modification, deletion, insertion, replay]

[117] [selection: modification, deletion, insertion, replay]

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

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

Note:

1. This SFR applies only for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.

9.1.3.12 FDP_RIP.1 (Subset residual information protection)

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from the following objects:

1. SCD

PACE / CA **2. Session Keys (immediately after closing related communication session)**

PACE 3. **the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret K)[118].**

The following data persistently stored by the TOE shall have the user data attribute "integrity checked persistent stored data":

1. SCD;
2. SVD (if persistently stored by the TOE).

The DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data".

Notes:

PACE CA 1. The SFR FPT_RIP.1.1 covers the definition in PP [BSI-CC-PP-0059-2009-MA-02] and extends it by PACE and CA aspects 2. and 3. These extensions do not conflict with the strict conformance to PP [BSI-CC-PP-0059-2009-MA-02].

PACE CA 2. The TOE shall destroy any session keys in accordance with FCS_CKM.4 after (i) detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication Protocol v.1. (iii) The TOE shall destroy the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys. (iv) The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA.

9.1.3.13 FDP_SDI.2/Persistent (Stored data integrity monitoring and action)

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

FDP_SDI.2.1/Persistent The TSF shall monitor user data stored in containers controlled by the TSF for integrity error 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:

1. prohibit the use of the altered data;
2. inform the S.Sigy about integrity error.

9.1.3.14 FDP_SDI.2/DTBS (Stored data integrity monitoring and action)

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

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

118 Is a [REFINEMENT]

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

FDP_SDI.2.2/DTBS	Upon detection of a data integrity error, the TSF shall: 1. prohibit the use of the altered data; 2. inform the S.Sigy about integrity error.

Note:

1. The integrity of TSF data like RAD shall be protected to ensure the effectiveness of the user authentication. This protection is a specific aspect of the security architecture (cf. ADV_ARC.1).

CGA

9.1.3.15 FDP_DAU.2/SVD (Data Authentication with Identity of Guarantor)

Hierarchical to:	FDP_DAU.1 Basic Data Authentication
Dependencies:	FIA_UID.1 Timing of identification
FDP_DAU.2.1/SVD	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of SVD.
FDP_DAU.2.2/SVD	The TSF shall provide CGA with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

Note:

1. This SFR only applies for the Life Cycle Phase “Usage/Operational” as the TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.

9.1.4 Identification and Authentication (FIA)

9.1.4.1 FIA_UID.1 (Timing of identification)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow: 1. self-test according to FPT_TST.1; PACE **2. carrying out the PACE protocol according to [ICAO-TR-110]** **3. performing of the Symmetric Authentication Mechanism[119]** on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Notes:

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

9.1.4.2 FIA_UAU.1 (Timing of authentication)

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FIA_UAU.1.1	The TSF shall allow: 1. self-test according to FPT_TST.1; 2. identification of the user by means of TSF required by FIA_UID.1;

CGA -

[119] [assignment: list of additional TSF mediated actions]

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

3. **establishing a trusted channel between the CGA and the TOE by means of TSF required by FTP_ITC.1/SVD,**

SCA 4. **establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD,**

PACE 5. **carrying out the PACE protocol according to [ICAO-TR-110]**

6. **performing of the Symmetric Authentication Mechanism[120]**

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

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

Notes:

1. This SFR has been amended with item (5) from [BSI-CC-PP-0068-V2-2011-MA-01] and with item (6) for authenticating the administrator before TOE personalization.
2. Item (3) of this SFR only applies for the Life Cycle Phase “Usage/Operational” as the TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.
3. Item (4) of this SFR applies only for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.
4. The user authenticated after a successfully performed PACE protocol is a PACE authenticated PACE Terminal. Please note that CAN does not effectively represent a secret (but other PACE passwords do so), but are restricted-revealable; i.e. it is either the legitimate user itself or an authorized other person or device (PACE Terminal).
5. After successful PACE authentication using the PIN.ADMIN R.Admin or the IT entity (CGA or SSCD Issuing Application) on its behalf is authenticated.

PACE

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. **PACE protocol according to [ICAO-TR-110],**
2. **Authentication Mechanism based on AES[121].**

Notes:

1. This SFR has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01].
2. This SFR covers the definition in [BSI-CC-PP-0068-V2-2011-MA-01]. The generation of random numbers (random nonce) used for the authentication protocol (PACE) as required by FIA_UAU.4/PACE is required by FCS_RND.1 from [BSI-CC-PP-0068-V2-2011-MA-01].
3. The authentication mechanism uses a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt.

PACE

9.1.4.4 FIA_UAU.5/PACE (Multiple authentication mechanisms)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/PACE The TSF shall provide:

1. **PACE protocol according to [ICAO-TR-110],**
2. **Passive Authentication according to [ICAO-9303-2015],**

[120] [assignment: list of additional TSF mediated actions]

[121] [assignment: identified authentication mechanism(s)]

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

3. **Secure Messaging in MAC-ENC mode according to [ICAO-TR-110],**
4. **Symmetric Authentication Mechanism based on AES,**
5. **The TOE accepts the authentication attempt by means of the Chip Authentication Protocol Version 1 only if Secure Messaging is established by PACE**[122]

to support user authentication.

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

1. **Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of Secure Messaging with the key agreed with the terminal by means of the PACE protocol.**
2. **The TOE accepts the authentication attempt as administrator by the symmetric authentication mechanism using an Administrator Personalization Key,**

CA 3. **After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1**[123]

Notes:

1. This SFR has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01]. Item (3) of FIA_UAU.5.2/PACE has been adapted from [BSI-CC-PP-0056-V2-2012-MA-02].
2. Please note that Passive Authentication does not authenticate any TOE's user, but provides evidence enabling an external entity (the terminal connected) to prove the origin of the TOE.

PACE

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/PACE The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal.**[124]

Notes:

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

CA

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/CA The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by R.Admin or the IT entity (CGA or SSCD Issuing Application) on its behalf.**[125]

[122] [assignment: list of multiple authentication mechanisms]

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

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

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

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

Notes:

1. This SFR has been adapted from the SFR FIA_UAU.6/EAC of [BSI-CC-PP-0056-V2-2012-MA-02].
2. The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [ICAO-9303-2015] include secure messaging for all commands exchanged after successful authentication of R.Admin or the IT entity (CGA or SSCD Issuing Application) on its behalf. The TOE checks by secure messaging in MAC_ENC mode each command based on a corresponding MAC algorithm whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user.

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

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1/Signature_Creation	The TSF shall re-authenticate the user under the conditions **1. Single signature** **S.Sigy before every single DTBS/R signature.** **2. Limited Mass signature** **S.Sigy before next signature after card reset or after Application QES was left or otherwise before (N+1)-th DTBS/R signature in a row when limit for consecutive signatures is N.** 3. **Unlimited Mass signature** **S.Sigy before next signature after card reset or after Application QES was left**[126].

Note:

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

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

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 *Timing of authentication*
FIA_AFL.1.1/RAD	The TSF shall detect when **an administrator configurable positive integer within 3 up to floor(MINLEN/2) (see note 3. below)**[127] unsuccessful authentication attempts occur related to consecutive failed authentication attempts.
FIA_AFL.1.2/RAD	When the defined number of unsuccessful authentication attempts has been met, the TSF shall block RAD **[REFINEMENT] of the signatory PIN (PIN.QES).**

Notes:

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

9.1.4.9 FIA_AFL.1/PIN (Authentication failure handling – for PINs other than the Signatory PIN)

Hierarchical to:	No other components.

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

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

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Dependencies:	FIA_UAU.1 *Timing of authentication*
FIA_AFL.1.1/PIN	The TSF shall detect when **3**[128] unsuccessful authentication attempts occur related to consecutive failed authentication attempts.
FIA_AFL.1.2/PIN	When the defined number of unsuccessful authentication attempts has been met, the TSF shall block ~~RAD~~ **PINs other than the signatory PIN (PIN.QES)[129].**

Note:

1. FIA_AFL.1/PIN is added to contents of PP [BSI-CC-PP-0059-2009-MA-02] (iterated).

PACE

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

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 *Timing of authentication*
FIA_AFL.1.1/PACE	The TSF shall detect when **1**[130] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts using the PACE password as the shared password**.[131]
FIA_AFL.1.2/PACE	When the defined number of unsuccessful authentication attempts has been **met[132],** the TSF shall **delay the next authentication attempt at least 6 seconds[133].**

Note:

1. FIA_AFL.1/PACE has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01].

PACE

9.1.4.11 FIA_AFL.1/Suspend_PIN (Authentication failure handling – Suspending PIN)

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 *Timing of authentication*
FIA_AFL.1.1/Suspend_PIN	The TSF shall detect when **2**[134] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts using the PACE password as the shared password for PACE[135]**.
FIA_AFL.1.2/Suspend_PIN	When the defined number of unsuccessful authentication attempts has been **met[136]**, the TSF shall **suspend the reference value of the PACE password according to [BSI-TR-03110-2-V221][137].**

Note:

1. FIA_AFL.1/Suspend_PIN has been adapted from [BSI-CC-PP-0086-2015], *PIN* has been changed to *PACE password*.

PACE

9.1.4.12 FIA_AFL.1/Block_PIN (Authentication failure handling – Blocking PIN)

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 *Timing of authentication*

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

129 Is a [REFINEMENT] of "RAD"

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

[131] [assignment: list of authentication events]

[132] [selection: met , surpassed]

[133] [assignment: list of actions]

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

[135] [assignment: list of authentication events]

[136] [selection: met , surpassed]

[137] [assignment: list of actions]

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

FIA_AFL.1.1/Block_PIN	The TSF shall detect when **1**[138] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts using the suspended**[139] **PACE password as the shared password for PACE**[140].
FIA_AFL.1.2/Block_PIN	When the defined number of unsuccessful authentication attempts has been **met**[141], the TSF shall **block the reference value of the PACE password according to [BSI-TR-03110-2-V221]**[142].

Note:

1. FIA_AFL.1/Block_PIN has been adapted from [BSI-CC-PP-0086-2015], *PIN* has been changed to *PACE password*.

PACE

9.1.4.13 FIA_AFL.1/AuthAdmin (Authentication failure handling – of administrator for personalization)

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 *Timing of authentication*
FIA_AFL.1.1/AuthAdmin	The TSF shall detect when **5**[143] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts**[144].
FIA_AFL.1.2/AuthAdmin	When the defined number of unsuccessful authentication attempts has been **met**[145], the TSF shall **delay the next authentication attempt at least 6 seconds**[146].

Note:

1. FIA_AFL.1/AuthAdmin is added to contents of PP [BSI-CC-PP-0059-2009-MA-02] (not iterated).
2. This SFR concerns the authentication of the administrator for personalization of the TOE using the Symmetric Authentication Mechanism with Administrator Personalization Key.

CGA

9.1.4.14 FIA_API.1 (Authentication proof of identity)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a **Chip Authentication Protocol Version 1 according to [BSI-TR-03110-1-V220]**[147] to prove the identity of the SSCD.

Note:

1. This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [BSI-TR-03110-1-V220]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [ICAO-9303-2015]. The terminal verifies by means of secure messaging whether the SSCD was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key.

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

[139] as required by FIA_AFL.1/Suspend_PIN

[140] [assignment: list of authentication events]

[141] [selection: met , surpassed]

[142] [assignment: list of actions]

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

[144] [assignment: list of authentication events]

[145] [selection: met , surpassed]

[146] [assignment: list of actions]

[147] [assignment: authentication mechanism]

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

9.1.5 Security Management (FMT)

9.1.5.1 FMT_SMR.1 (Security roles)

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FMT_SMR.1.1	The TSF shall maintain the roles R.Admin and R.Sigy **and PACE Terminal**[148].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

9.1.5.2 FMT_SMF.1 (Security management functions)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: 1) creation and modification of RAD; 2) enabling the signature creation function; 3) modification of the security attribute SCD/SVD management, SCD operational; 4) change the default value of the security attribute SCD Identifier; 5) **none**[149].

9.1.5.3 FMT_MOF.1 (Management of security functions behavior)

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1	The TSF shall restrict the ability to enable the functions signature creation function to R.Sigy.

9.1.5.4 FMT_MSA.1/Admin (Management of security attributes)

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1/Admin	The TSF shall enforce the SCD/SVD_Generation_SFP to restrict the ability to modify **and none**[150] the security attributes SCD/SVD management to R.Admin.

9.1.5.5 FMT_MSA.1/Signatory (Management of security attributes)

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1/Signatory	The TSF shall enforce the Signature_Creation_SFP to restrict the ability to modify the security attributes SCD operational to R.Sigy.

[148] is a [REFINEMENT] of [assignment: *the authorised identified roles*]

[149] [assignment: list of other security management functions to be provided by the TSF]

[150] [assignment: other operations]

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

9.1.5.6 FMT_MSA.2 (Secure security attributes)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for SCD/SVD Management and SCD operational.

Security attribute "SCD/SVD Management" can only have the values "authorized" or "not authorized". Both values are secure, depending on the situation.

Security attribute "SCD operational" can only have the values "no" or "yes". Both values are secure, depending on the situation.

The security attribute values are not secure by themselves but in combinations.

The secure values of the combinations are shown in the following table:

SCD/SVD Management	SCD operational	Secure
authorized	yes	YES
authorized	no	YES
not authorized	yes	YES
not authorized	no	YES

Table 9-2: Secure values of the combinations of security attributes

Therefore all combinations can be seen as secure[151].

9.1.5.7 FMT_MSA.3 (Static attribute initialization)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the SCD/SVD_Generation_SFP, SVD_Transfer_SFP and Signature_Creation_SFP 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.

9.1.5.8 FMT_MSA.4 (Security attribute value inheritance)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes:

1) If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute “SCD operational of the SCD” shall be set to “no” as a single operation.

2) ~~If S.Sigy successfully generates an SCD/SVD pair the security attribute “SCD operational of the SCD” shall be set to “yes” as a single operation.~~

Note:

[151] is a [REFINEMENT]

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

1. Rule (2) is deleted, as the TOE does not support generating an SVD/SCD pair by the signatory alone.

9.1.5.9 FMT_MTD.1/RAD (Management of TSF data)

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/RAD	The TSF shall restrict the ability to create the RAD **[REFINEMENT] of the Signatory once** to ~~R.Admin~~ **R.Sigy only after successful authentication with the transport PIN (PIN.T)**[152].

Note:

1. FMT_MTD.1/RAD amounts to requirement "FMT_MTD.1/Admin".

9.1.5.10 FMT_MTD.1/Signatory (Management of TSF data)

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/Signatory	The TSF shall restrict the ability to modify **or unblock**[153] the RAD to R.Sigy.

PACE

9.1.5.11 FMT_MTD.1/KEY_READ (Management of TSF data)

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions **fulfilled by FMT_SMF.1** FMT_SMR.1 Security roles **fulfilled by FMT_SMR.1**
FMT_MTD.1.1/KEY_READ	The TSF shall restrict the ability to **read**[154] the **1. PACE passwords,** **2. Chip Authentication private key,** 3. **Electronic signature key** 4. **Administrator Personalization Key**[155] to **none**[156].

Note:

1. This SFR has been adapted from [BSI-CC-PP-0068-V2-2011-MA-01], with Item (2) “Personalization Agent Keys” removed.

PACE

9.1.5.12 FMT_MTD.1/CAPK (Management of TSF data - Chip Authentication Private Key)

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/KEY_READ	The TSF shall restrict the ability to **load**[157] the **Chip Authentication Private Key**[158] to **R.Admin**[159] **[REFINEMENT] before issuing the TOE**.

[152] is a [REFINEMENT] of “R.Admin”

[153] [assignment: other operations]

[154] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]

[155] [assignment: list of TSF data]

[156] [assignment: the authorised identified roles]

[157] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]

[158] [assignment: list of TSF data]

[159] [assignment: the authorised identified roles]

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

Notes:

1. This SFR has been adapted from [BSI-CC-PP-0056-V2-2012-MA-02].
2. [BSI-CC-PP-0056-V2-2012-MA-02]The verb “load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory.
3. The Chip Authentication Private Key mentioned here is used for performing **Chip Authentication Protocol Version 1**.

9.1.6 Protection of the TSF (FPT)

9.1.6.1 FPT_EMS.1/SSCD (TOE Emanation of SCD and RAD)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1/SSCD The TOE shall not emit

1) **shape and amplitude of signals,**
2) **time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines**
3) **during internal operations or data transmissions**[160]

in excess of **unintelligible limits**[161] enabling access to RAD and SCD.

FPT_EMS.1.2/SSCD The TSF shall ensure **any users**[162] are unable to use the following interface **TOE’s contactless/contact interface and circuit contacts**[163] to gain access to RAD and SCD.

Note:

1. FPT_EMS.1/SSCD amounts to requirement "FPT_EMS.1".

PACE CA

9.1.6.2 FPT_EMS.1/KEYS (TOE Emanation of secret/private keys)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1/KEYS The TOE shall not emit

1) **shape and amplitude of signals,**
2) **time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines**
3) **during internal operations or data transmissions**[164]

in excess of **unintelligible limits**[165] enabling access to

1. **PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}),**
2. **the ephemeral private key ephem-SK_{PICC}-PACE,**
3. **Chip Authentication private key**
4. **Administrator Personalization Key**

[160] [assignment: types of emissions]

[161] [assignment: specified limits]

[162] [assignment: type of users]

[163] [assignment: type of connection]

[164] [assignment: types of emissions]

[165] [assignment: specified limits]

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

5. **Chip Authentication session keys (CA-K_{MAC}, CA-K_{Enc})**[166]

and

6. **none**[167].

FPT_EMS.1.2/KEYS The TSF shall ensure **any users**[168] are unable to use the following interface **TOE's contactless/contact interface and circuit contacts**[169] to gain access to

1. **PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}),**
2. **the ephemeral private key ephem-SK_{PICC}-PACE,**
3. **Chip Authentication private key**
4. **Administrator Personalization Key**
5. **Chip Authentication session keys (CA-K_{MAC}, CA-K_{Enc})**[170]

and

6. **none**[171].

Notes:

1. FPT_EMS.1/KEYS has been adapted from "FPT_EMS.1".of [BSI-CC-PP-0068-V2-2011-MA-01]. The SFRs FPT_EMS.1.1/KEYS and FPT_EMS.1.2/KEYS are extended by CA aspects 3., 4. and 5.
2. The Chip Authentication private key is stored in the TOE according to FMT_MTD.1/CAPK.

9.1.6.3 FPT_FLS.1 (Failure with preservation of secure state)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

1. self-test according to FPT_TST fails;
2. **Failures during cryptographic operations**
3. **Memory failures during TOE execution**
4. **Out of range failures of temperature, clock and voltage sensors**
5. **Failures during random number generation**[172]**.**

9.1.6.4 FPT_PHP.1 (Passive detection of physical attack)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

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

9.1.6.5 FPT_PHP.3 (Resistance to physical attack)

Hierarchical to: No other components.

Dependencies: No dependencies.

---

[166] [assignment: list of types of TSF data]

[167] [assignment: list of types of user data]

[168] [assignment: type of users]

[169] [assignment: type of connection]

[170] [assignment: list of types of TSF data]

[171] [assignment: list of types of user data]

[172] [assignment: list of other types of failures in the TSF]

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

FPT_PHP.3.1 The TSF shall resist **physical manipulation and physical probing**[173] to the **TSF**[174] by responding automatically such that the SFRs are always enforced.

Note:

1. The TOE implements appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSF could not be violated at any time. Hence, 'automatic response' means here
   i. assuming that there might be an attack at any time and
   ii. countermeasures are provided at any time.

9.1.6.6 FPT_TST.1 (TSF testing)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self-tests **during initial start-up and at the conditions**

1. **Generation of the SCD/SVD key pair according to "FCS_CKM.1/EC" or "FCS_CKM.1/RSA"**
2. **Signature-creation according to "FCS_COP.1/EC" or "FCS_COP.1/RSA"**
3. **VAD verification**
4. **RAD modification**[175]

to demonstrate the correct operation of the TSF.

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

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

9.1.7 Trusted Path/Channels (FTP)

CGA

9.1.7.1 FTP_ITC.1/SVD (Inter-TSF trusted channel)

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/SVD The TSF shall provide a communication channel between itself and another trusted IT product CGA that is logically distinct from other communication channels and provides ensured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SVD The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3/SVD The TSF or the CGA shall initiate communication via the trusted channel for

1. data Authentication with Identity of Guarantor according to FIA_API.1 and FDP_DAU.2/SVD,
2. **none**[176].

Note:

[173] [assignment: physical tampering scenarios]

[174] [assignment: list of TSF devices/elements]

[175] [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self-test should occur]]

[176] [assignment: list of other functions for which a trusted channel is required]

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

1. This SFR only applies for the Life Cycle Phase “Usage/Operational” as the TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.

SCA

9.1.7.2 FTP_ITC.1/VAD (Inter-TSF trusted channel – TC Human Interface Device)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/VAD	The TSF shall provide a communication channel between itself and another trusted IT product HID that is logically distinct from other communication channels and provides ensured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/VAD	The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/VAD	The TSF or the HID shall initiate communication via the trusted channel for 1. User authentication according to FIA_UAU.1, 2. **none**[177].

Notes:

2. The PACE protocol used for authentication is a zero-knowledge protocol and thus protects the confidentiality of the VAD implicitly.
3. This SFR applies only for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.

SCA

9.1.7.3 FTP_ITC.1/DTBS (Inter-TSF trusted channel – Signature creation Application)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/DTBS	The TSF shall provide a communication channel between itself and another trusted IT product SCA that is logically distinct from other communication channels and provides ensured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/DTBS	The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/DTBS	The TSF or the SCA shall initiate communication via the trusted channel for 1. signature creation, 2. **none**[178].

Note:

1. This SFR applies only for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.

[177] [assignment: list of other functions for which a trusted channel is required]

[178] [assignment: list of other functions for which a trusted channel is required]

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

9.2 TOE Security Assurance Requirements

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Table 9-3: Security assurance requirements: EAL4 augmented with ALC_DVS.2 and AVA_VAN.5

9.3 Security Requirements Rationale

9.3.1 Security Requirements Coverage

Security objectives and security functional requirements that are added by **PP SSCD KG TCCGA** or **PP SSCD KG TCSCA** are color coded for better readability. Security functional requirements taken from [BSI-CC-PP-0056-V2-2012-MA-02] or [BSI-CC-PP-0068-V2-2011-MA-01] or modified to meet those PPs, respectively, are given in italics, security functional requirements taken from [BSI-CC-PP-0086-2015] are given in **bold face**.

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	**OT.TOE_SSCD_Auth**	**OT.TOE_TC_SVD_Exp**	**OT.TOE_TC_VAD_Imp**	**OT.TOE_TC_DTBS_Imp**
FCS_CKM.1/EC	x		x	x	x										
FCS_CKM.1/RSA	x		x	x	x										
FCS_CKM.1/DH_PACE	x						x						x	x	x
FCS_CKM.1/CA	x												x		
FCS_CKM.4	x				x								x	x	x
FCS_COP.1/EC	x					x									
FCS_COP.1/RSA	x					x									
FCS_COP.1/SHA						x									

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
FCS_COP.1/PACE_ENC	x						x						x	x	x
FCS_COP.1/PACE_MAC	x						x						x	x	x
FCS_COP.1/CA_ENC	x												x		
FCS_COP.1/CA_MAC	x												x		
FCS_COP.1/AES_MAC	x														
FCS_RNG.1	x						x						x	x	x
FDP_ACC.1/TRM	x												x		
FDP_ACF.1/TRM	x												x		
FDP_ACC.1/ SCD/SVD_Generation	x	x													
FDP_ACF.1/ SCD/SVD_Generation	x	x													
FDP_ACC.1/ SVD_Transfer	x												x		
FDP_ACF.1/ SVD_Transfer	x												x		
FDP_ACC.1/ Signature_Creation	x						x								
FDP_ACF.1/ Signature_Creation	x						x								
FDP_UCT.1/TRM	x						x						x	x	x
FDP_UIT.1/TRM	x						x						x	x	x
FDP_UIT.1/DTBS															x
FDP_RIP.1					x		x								
FDP_SDI.2/Persistent				x	x	x									
FDP_SDI.2/DTBS							x	x							
FDP_DAU.2/SVD													x		
FIA_UID.1[179]	x	x					x						x	x	x
FIA_UAU.1[180]	x	x					x					x	x	x	x
FIA_UAU.4/PACE	x						x						x	x	x
FIA_UAU.5/PACE	x						x						x	x	x
FIA_UAU.6/PACE	x						x						x	x	x
FIA_UAU.6/CA	x												x		
FIA_UAU.6/ Signature_Creation							x								
FIA_AFL.1/RAD							x								
FIA_AFL.1/PIN							x								
FIA_AFL.1/PACE							x								
FIA_AFL.1/ Suspend_PIN							x								
FIA_AFL.1/Block_PIN							x								
FIA_AFL.1/AuthAdmin	x														
FIA_API.1	x											x			
FMT_SMR.1	x						x								
FMT_SMF.1	x			x			x								
FMT_MOF.1	x						x								
FMT_MSA.1/Admin	x	x													
FMT_MSA.1/Signatory	x						x								

[179] This SFR is amended with an item from [BSI-CC-PP-0068-V2-2011-MA-01].

[180] This SFR is amended with items from **PP SSCD KG TCCGA**, **PP SSCD KG TCSCA** and [BSI-CC-PP-0068-V2-2011-MA-01].

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
FMT_MSA.2	x	x					x								
FMT_MSA.3	x	x					x								
FMT_MSA.4	x	x		x			x								
FMT_MTD.1/RAD	x						x								
FMT_MTD.1/Signatory	x						x								
FMT_MTD.1/KEY_READ	x												x	x	x
FMT_MTD.1/CAPK	x											x	x		
FPT_EMS.1/SSCD					x				x						
FPT_EMS.1/KEYS									x		x				
FPT_FLS.1					x										
FPT_PHP.1										x					
FPT_PHP.3					x						x				
FPT_TST.1	x				x	x									
FTP_ITC.1/SVD													x		
FTP_ITC.1/VAD														x	
FTP_ITC.1/DTBS															x

Table 9-4: Functional Requirement to TOE security objective mapping

9.3.2 TOE Security Requirements Sufficiency

OT.Lifecycle_Security (Life cycle security) is provided by the SFRs

- FCS_CKM.1/EC (for EC SCD/SVD generation),
- FCS_CKM.1/RSA (for RSA SCD/SVD generation),
- FCS_COP.1/EC (for SCD usage using EC),
- FCS_COP.1/RSA (for SCD usage using RSA) and
- FCS_CKM.4 (for SCD destruction)

ensuring cryptographically secure life cycle of the SCD.

The SCD/SVD generation is controlled by TSF according to

- FDP_ACC.1/SCD/SVD_Generation and
- FDP_ACF.1/SCD/SVD_Generation.

The SVD transfer for certificate generation is controlled by TSF according to

- FDP_ACC.1/SVD_Transfer and
- FDP_ACF.1/SVD_Transfer.

The SCD usage is ensured by access control

- FDP_ACC.1/Signature_Creation,
- FDP_ACF.1/Signature_Creation,

which is based on the security attribute secure TSF management according to

- FMT_MOF.1,
- FMT_MSA.1/Admin,

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

- FMT_MSA.1/Signatory,
- FMT_MSA.2,
- FMT_MSA.3,
- FMT_MSA.4,
- FMT_MTD.1/RAD,
- FMT_MTD.1/Signatory,
- FMT_SMF.1 and
- FMT_SMR.1.

The test functions

- FPT_TST.1

provides failure detection throughout the life cycle.

(Life cycle security) in the Phase “Usage/Preparation” is provided by the SFRs

- FCS_COP.1/AES_MAC,
- FIA_UID.1,
- FIA_UAU.1,
- FIA_AFL.1/AuthAdmin provides protection against brute force attacks against authentication.

(Life cycle security) in the Phase “Usage/Operational” is provided by the SFRs

- FCS_CKM.1/DH_PACE,
- FCS_CKM.1/CA,
- FCS_CKM.4 (for session key destruction),
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_COP.1/CA_ENC,
- FCS_COP.1/CA_MAC,
- FCS_RNG.1,
- FDP_ACC.1/TRM,
- FDP_ACF.1/TRM,
- FIA_UID.1,
- FIA_UAU.1,
- FIA_UAU.4/PACE,
- FIA_UAU.5/PACE,
- FIA_UAU.6/PACE,
- FIA_UAU.6/CA,
- FIA_API.1,
- FMT_MTD.1/KEY_READ,
- FMT_MTD.1/CAPK.

OT.SCD/SVD_Auth_Gen (Authorized SCD/SVD generation) addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by

- FIA_UID.1 and
- FIA_UAU.1

provide user identification and user authentication prior to enabling access to authorized functions. The SFR

- FDP_ACC.1/SCD/SVD_Generation and

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

- FDP_ACF.1/SCD/SVD_ Generation

provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by

- FMT_MSA.1/Admin,
- FMT_MSA.2 and
- FMT_MSA.3

for static attribute initialization. The SFR

- FMT_MSA.4

defines rules for inheritance of the security attribute “SCD operational” of the SCD.

OT.SCD_Unique (Uniqueness of the signature creation data) implements the requirement of practically unique SCD as laid down in Annex III of the Directive, paragraph 1(a), which is provided by the cryptographic algorithms specified by

- FCS_CKM.1/EC and
- FCS_CKM.1/RSA.

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by

- FCS_CKM.1/EC and
- FCS_CKM.1/RSA

to generate corresponding SVD/SCD pairs. The security functions specified by

- FDP_SDI.2/Persistent

ensure that the keys are not modified, so to retain the correspondence. Moreover, the SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. The management functions identified by

- FMT_SMF.1 and by
- FMT_MSA.4

allow R.Admin to modify the default value of the security attribute SCD Identifier.

OT.SCD_Secrecy (Secrecy of signature creation data) is provided by the security functions specified by the following SFRs.

- FCS_CKM.1/EC and
- FCS_CKM.1/RSA

ensure the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD.

The security functions specified by

- FDP_RIP.1 and
- FCS_CKM.4

ensure that residual information on SCD is destroyed after the SCD has been used for signature creation and that destruction of SCD leaves no residual information.

The security functions specified by

- FDP_SDI.2/Persistent

ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD.

- FPT_TST.1

tests the working conditions of the TOE and

- FPT_FLS.1

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA).

- FPT_EMS.1/SSCD and
- FPT_PHP.3

require additional security features of the TOE to ensure the confidentiality of the SCD.

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by

- FCS_COP.1/EC,
- FCS_COP.1/RSA **and**
- FCS_COP.1/SHA

which ensures the cryptographic robustness of the signature algorithms,

- FDP_SDI.2/Persistent

corresponds to the integrity of the SCD implemented by the TOE and

- FPT_TST.1

ensures self-tests ensuring correct signature creation.

FCS_COP.1/SHA is used before FCS_COP.1/EC and FCS_COP.1/RSA if DTBS or an intermediate hash value with the remainder of DTBS (last round hash value) is sent to the TOE for signature creation.

OT.Sigy_SigF (Signature creation function for the legitimate signatory only) is provided by an SFR for identification, authentication and access control.

- FIA_UAU.1 and
- FIA_UID.1

ensure that no signature creation function can be invoked before the signatory is identified and authenticated.

The security functions specified by

- FMT_MTD.1/RAD and
- FMT_MTD.1/Signatory

manage the authentication function.

- FIA_AFL.1/RAD and
- FIA_AFL.1/PIN

provide protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.

- FIA_AFL.1/PACE provides protection against brute force attacks against authentication.
- FIA_AFL.1/Suspend_PIN provides protection against denial-of-service attacks.
- FIA_AFL.1/Block_PIN provides protection against brute force attacks against authentication.

The security functions specified by

- FDP_SDI.2/DTBS

ensures the integrity of stored DTBS and

- FDP_RIP.1

prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process).

The security functions specified by

- FDP_ACC.1/Signature_Creation and
- FDP_ACF.1/Signature_Creation

provide access control based on the security attributes managed according to the SFRs

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

- FMT_MTD.1/Signatory,
- FMT_MSA.2,
- FMT_MSA.3 and
- FMT_MSA.4.

The SFRs

- FMT_SMF.1 and
- FMT_SMR.1

list these management functions and the roles. These ensure that the signature process is restricted to the signatory.

- FMT_MOF.1

restricts the ability to enable the signature creation function to the signatory.

- FMT_MSA.1/Signatory

restricts the ability to modify the security attributes SCD operational to the signatory.

In the Phase “Usage/Operational” Signature creation function for the legitimate signatory only is additionally provided by the SFRs

- FCS_CKM.1/DH_PACE,
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_RNG.1,
- FDP_UCT.1/TRM,
- FDP_UIT.1/TRM,
- FIA_UID.1,
- FIA_UAU.1,
- FIA_UAU.4/PACE,
- FIA_UAU.5/PACE and
- FIA_UAU.6/PACE.

OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) ensures that the DTBS/R is not altered by the TOE. The integrity functions specified by

- FDP_SDI.2/DTBS

require that the DTBS/R has not been altered by the TOE.

OT.EMSEC_Design (Provide physical emanations security) covers that no intelligible information is emanated. This is provided by

- FPT_EMS.1.1/SSCD and
- FPT_EMS.1.1/KEYS.

OT.Tamper_ID (Tamper detection) is provided by

- FPT_PHP.1

by the means of passive detection of physical attacks.

OT.Tamper_Resistance (Tamper resistance) is provided by

- FPT_EMS.1.1/KEYS and

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

- FPT_PHP.3

to resist physical attacks.

CGA **OT.TOE_SSCD_Auth** (Authentication proof as SSCD) requires the TOE to provide security mechanisms to identify and to authenticate themselves as SSCD[181], which is directly provided by

- FIA_API.1.

The SFR

- FIA_UAU.1

allows (additionally to PP SSCD KG) establishment of the trusted channel before (human) user is authenticated.

Furthermore

- FMT_MTD.1/CAPK

provides the Chip Authentication private key.

CGA **OT.TOE_TC_SVD_Exp** (TOE trusted channel for SVD export) requires the TOE to provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA[182], which is directly provided by

- the SVD transfer for certificate generation controlled by TSF according to
  - FDP_ACC.1/SVD_Transfer and
  - FDP_ACF.1/SVD_Transfer.
- The SFR
  - FDP_DAU.2/SVD

  requires the TOE to provide CGA with the ability to verify evidence of the validity of the SVD and the identity of the user that generated the evidence.
- The SFR
  - FTP_ITC.1/SVD

  requires the TOE to provide a trusted channel to the CGA.

The functionality for integrity and confidentiality is provided by

- FCS_CKM.1/DH_PACE,
- FCS_CKM.1/CA,
- FCS_CKM.4 (for session key destruction),
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_COP.1/CA_ENC,
- FCS_COP.1/CA_MAC,
- FCS_RNG.1,
- FDP_ACC.1/TRM,
- FDP_ACF.1/TRM,
- FDP_UCT.1/TRM,
- FDP_UIT.1/TRM,
- FIA_UID.1,
- FIA_UAU.1,

[181] This security objective only applies in case a communication channel to the CGA (via trusted channel) in the Life Cycle Phase “Usage/Operational” is needed.

[182] The TOE 'CardOS DI V5.4 QES Version 1.0' provides a communication channel to the CGA (via trusted channel) only in the Life Cycle Phase “Usage/Operational”.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

- FIA_UAU.4/PACE,
- FIA_UAU.5/PACE,
- FIA_UAU.6/PACE,
- FIA_UAU.6/CA,
- FMT_MTD.1/KEY_READ and
- FMT_MTD.1/CAPK.

FDP_RIP.1 requires erasing the values of session keys

SCA **OT.TOE_TC_VAD_Imp** (Trusted channel of TOE for VAD import) is provided by

- FTP_ITC.1/VAD

to provide a trusted channel to protect the VAD provided by the HID to the TOE.

The functionality for integrity and confidentiality is provided by

- FCS_CKM.1/DH_PACE,
- FCS_CKM.4 (for session key destruction),
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_RNG.1,
- FDP_UCT.1/TRM,
- FDP_UIT.1/TRM,
- FIA_UAU.1,
- FIA_UAU.4/PACE,
- FIA_UAU.5/PACE,
- FIA_UAU.6/PACE and
- FMT_MTD.1/KEY_READ.

FDP_RIP.1 requires erasing the values of session keys

SCA **OT.TOE_TC_DTBS_Imp** (Trusted channel of TOE for DTBS) is provided by

- FTP_ITC.1/DTBS

to provide a trusted channel to protect the DTBS provided by the SCA to the TOE and by

- FDP_UIT.1/DTBS

which requires the TSF to verify the integrity of the received DTBS.

The functionality for integrity and confidentiality is provided by

- FCS_CKM.1/DH_PACE,
- FCS_CKM.4 (for session key destruction),
- FCS_COP.1/PACE_ENC,
- FCS_COP.1/PACE_MAC,
- FCS_RNG.1,
- FDP_UCT.1/TRM,
- FDP_UIT.1/TRM,
- FIA_UAU.1,
- FIA_UAU.4/PACE,

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

- FIA_UAU.5/PACE,
- FIA_UAU.6/PACE and
- FMT_MTD.1/KEY_READ.

FDP_RIP.1 requires erasing the values of session keys

The security objective OT.Data_Integrity aims that the TOE always ensures integrity of the User and TSF-data stored and, after the PACE authentication, of these data exchanged (physical manipulation and unauthorised modifying). Physical manipulation is addressed by FPT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1, FDP_ACF.1). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. Unauthorised modifying of the exchanged data is addressed, in the first line, by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC). The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords.

9.3.2.1 Different possibilities to create signatures

Note:

1. This chapter is added to contents of PP [BSI-CC-PP-0059-2009-MA-02].

With the security functions specified by

- FDP_ACC.1/Signature_Creation and
- FDP_ACF.1/Signature_Creation

the TOE ensures only following possibilities to create signatures:

1. The signatory alone signs one **DTBS/R** with Signature_Creation_SFP (FMT_MOF.1)
2. The signatory alone signs a limited number of **DTBS/R**s with Signature_Creation_SFP in a row (FMT_MOF.1)
3. The signatory alone signs an unlimited number of **DTBS/R**s with Signature_Creation_SFP in a row (FMT_MOF.1)

9.3.2.2 Different reasons for authentication

Note:

1. This chapter is added to contents of PP [BSI-CC-PP-0059-2009-MA-02].

OT.Sigy_SigF (Signature creation function for the legitimate signatory only) is ensured by re-authentication according to

- FIA_UAU.6/Signature_Creation

as follows:

1. S.Sigy
   a) before every single **DTBS/R** signature

   if S.Sigy is allowed to create a single signature.
2. S.Sigy
   a) before next signature after card reset or
   b) after Application QES was left or
   c) otherwise before (N+1)-th **DTBS/R** signature in a row when limit for consecutive signatures is N

   if S.Sigy is allowed to create a limited number of mass signatures in a row.
3. S.Sigy
   a) before next signature after card reset or
   b) after Application QES was left

   if S.Sigy is allowed to create an unlimited number of mass signatures in a row.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

9.3.3 Satisfaction of Dependencies of Security Requirements

Functional requirements	Dependencies	Satisfied by
FCS_CKM.1/EC	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/EC, FCS_CKM.4
FCS_CKM.1/RSA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/RSA, FCS_CKM.4
FCS_CKM.1/DH_PACE	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_CKM.4
FCS_CKM.1/ CA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/EC, FCS_CKM.1/RSA, FCS_CKM.1/DH_PACE
FCS_COP.1/EC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/EC, FCS_CKM.4
FCS_COP.1/RSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/RSA, FCS_CKM.4
FCS_COP.1/SHA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	are not fulfilled but justified: see note (1) below
FCS_COP.1/PACE_ENC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/DH_PACE, FCS_CKM.4
FCS_COP.1/PACE_MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/DH_PACE, FCS_CKM.4
FCS_COP.1/CA_ENC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/CA_MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/CA, FCS_CKM.4
FCS_COP.1/AES_MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	not fulfilled but justified: see note (2) below, FCS_CKM.4
FCS_RNG.1	No dependencies	n/a
FDP_ACC.1/TRM	FDP_ACF.1	FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/TRM, FMT_MSA.3
FDP_ACC.1/ SCD/SVD_Generation	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation
FDP_ACF.1/ SCD/SVD_Generation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FDP_ACC.1/ SVD_Transfer	FDP_ACF.1	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/ SVD_Transfer	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDP_ACC.1/ Signature_Creation	FDP_ACF.1	FDP_ACF.1/Signature_Creation
FDP_ACF.1/ Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_UCT.1/TRM	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1/SVD, FTP_ITC.1/VAD, FTP_ITC.1/DTBS, FDP_ACC.1/TRM
FDP_UIT.1/TRM	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1/SVD, FTP_ITC.1/VAD, FTP_ITC.1/DTBS, FDP_ACC.1/TRM
FDP_UIT.1/DTBS	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1]	FDP_ACC.1/Signature_Creation, FTP_ITC.1/DTBS
FDP_RIP.1	No dependencies	n/a
FDP_SDI.2/Persistent	No dependencies	n/a
FDP_SDI.2/DTBS	No dependencies	n/a
FDP_DAU.2/SVD	FIA_UID.1	FIA_UID.1
FIA_UID.1[183]	No dependencies	n/a

[183] This SFR is amended with an item from [BSI-CC-PP-0068-V2-2011-MA-01].

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Functional requirements	Dependencies	Satisfied by
FIA_UAU.1[184]	FIA_UID.1	FIA_UID.1
FIA_UAU.4/PACE	No dependencies	n/a
FIA_UAU.5/PACE	No dependencies	n/a
FIA_UAU.6/PACE	No dependencies	n/a
FIA_UAU.6/CA	No dependencies	n/a
FIA_AFL.1/RAD	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/PIN	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/PACE	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/ Suspend_PIN	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/Block_PIN	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1/AuthAdmin	FIA_UAU.1	FIA_UAU.1
FIA_API.1	No dependencies	n/a
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FMT_SMF.1	No dependencies	n/a
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation
FMT_MTD.1/RAD	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/KEY_READ	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/CAPK	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FPT_EMS.1/SSCD	No dependencies	n/a
FPT_EMS.1/KEYS	No dependencies	n/a
FPT_FLS.1	No dependencies	n/a
FPT_PHP.1	No dependencies	n/a
FPT_PHP.3	No dependencies	n/a
FPT_TST.1	No dependencies	n/a
FTP_ITC.1/SVD	No dependencies	n/a
FTP_ITC.1/VAD	No dependencies	n/a
FTP_ITC.1/DTBS	No dependencies	n/a

Table 9-5: Satisfaction of dependencies of security functional requirements

Note:

1. Justification of “FCS_COP.1/SHA” can be found in “9.1.2.8 FCS_COP.1/SHA (Cryptographic operation – Hash calculation”.
2. Justification of “FCS_COP.1/AES_MAC” can be found in “9.1.2.13 FCS_COP.1/AES_MAC (Cryptographic operation – MACing with AES) ”

[184] This SFR is amended with items from **PP SSCD KG TCCGA**, **PP SSCD KG TCSCA** and [BSI-CC-PP-0068-V2-2011-MA-01].

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

Assurance requirement(s)	Dependencies	Satisfied by
EAL4 package	(dependencies of EAL4 package are not reproduced here)	By construction, all dependencies are satisfied in a CC EAL package
ALC_DVS.2	no dependencies	
AVA_VAN.5	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1 (all are included in EAL4 package)

Table 9-6: Satisfaction of dependencies of security assurance requirements

9.3.4 Rationale for Chosen Security Assurance Requirements

The assurance level for PP SSCD KG, PP SSCD KG TCCGA and PP SSCD KG TCSCA is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this ST is just such a product. Augmentation results from the selection of:

ALC_DVS.2 Sufficiency of security measures

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.

The requirements of the claimed protection profiles are met or exceeded and the dependencies are fulfilled as shown in Table 9-6.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

10 TOE Summary Specification (ASE_TSS)

This chapter describes the TOE security functions and the assurance measures covering the requirements of the previous chapter.

10.1 TOE Security Functions

This chapter gives the overview description of the different TOE security functions composing the TSF.

10.1.1 SF_HardwareCryptoLibrary

This security function covers the security functions of the hardware (**IC**) as well as of the cryptographic libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010. The Security Target of the hardware [Infineon-ST-M7892-D11-G12] defines the following security features:

- SF_DPM Device Phase Management
- SF_PS Protection against Snooping
- SF_PMA Protection against Modification Attacks
- SF_PLA Protection against Logical Attacks
- SF_CS Cryptographic Support
- SF_MAE Mutual Authentication Extension

10.1.2 SF_UserIdentificationAuthentication

This security function is responsible for the identification and authentication of the user roles (FMT_SMR.1)

- Administrator
- Signatory
- PACE Terminal

by the methods:

- PACE authentication method[185] according to [BSI-TR-03110-1-V220] and [BSI-TR-03110-2-V221] (FIA_UID.1.1(2), FIA_UAU.1.1(5) and FIA_UAU.5/PACE)
  - It uses
    a) PIN.CH,
    b) optionally PUK.CH,
    c) PIN.T,
    d) PIN.ADMIN or
    e) CAN as passwords.
  - In the first step of the method a random nonce (FCS_RNG.1) encrypted with the password using the cryptographic algorithm AES is transmitted from the TOE to a terminal (FIA_UAU.4/PACE).
  - The method is configured to set the card to a **suspended state** before the password is finally blocked (only PIN.CH, PUK.CH, PIN.T and PIN.ADMIN) (FIA_AFL.1/Suspend_PIN and FIA_AFL.1/Block_PIN) or to **delay the processing** of the authentication command after a failed authentication (CAN) (FIA_AFL.1/PACE).

[185] The PACE authentication method is only applicable in cases where the communication between the TOE and another entity via trusted channel is mandatory.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

- The cryptographic method for confidentiality is AES/CBC (supplied by SF_HardwareCryptoLibrary) (FCS_COP.1/PACE_ENC).
- The cryptographic method for authenticity is CMAC (supplied by SF_HardwareCryptoLibrary) (FCS_COP.1/PACE_MAC).
- On error (wrong MAC, wrong challenge) the user role is not identified/authenticated.
- A usage counter of 64 prevents the unlimited usage of PUK.CH.
- On success the session keys are created and stored for Secure Messaging (FCS_CKM.1/DH_PACE).
- Keys and data in transient memory are overwritten after usage (FCS_CKM.4).

- Secure Messaging (FIA_UAU.1.1(3), FIA_UAU.1.1(4) and FIA_UAU.5/PACE)
  - The cryptographic method for confidentiality is AES/CBC (supplied by SF_HardwareCryptoLibrary (FCS_COP.1/PACE_ENC, FCS_COP.1/CA_ENC).
  - The cryptographic method for authenticity is CMAC (supplied by SF_HardwareCryptoLibrary) (FCS_COP.1/PACE_MAC, FCS_COP.1/CA_MAC).
  - In a Secure Messaging protected command the method for confidentiality and the method for authenticity must be present.
  - A session key is used.
  - Any command protected correctly with the session keys is considered to be sent by the successfully authenticated user (FIA_UAU.6/PACE, FIA_UAU.6/CA).
  - On any command that is not protected correctly with the session keys these are overwritten and a new PACE authentication is required.
  - Keys and data in transient memory are overwritten after usage (FCS_CKM.4).
- PIN authentication mechanism using
  - the PIN for qualified signature (PIN.QES) as PIN
    - PIN.QES is a password with a minimum length of 6 digits for authentication data that is blocked after an administrator configurable positive integer within 3 up to floor(MINLEN/2) consecutive failed authentication attempts (FIA_AFL.1/RAD)
    - The transmission of the PIN.QES must be protected by Secure Messaging with PACE for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.
  - the transport PIN (PIN.T) as PIN
    - PIN.T is a password with a minimum length of 5 digits for authentication data that is blocked after 3 consecutive failed authentication attempts (FIA_AFL.1/PIN)
    - The transport PIN (PIN.T) can be used as PIN for the PIN authentication mechanism for the configuration TC-SCA-CL-Only for contact-based communication only.
  - the optional personal unblocking key (PUK.CH) as PIN
    - PUK.CH is a password with a minimum length of 8 digits for authentication data that is blocked after 3 consecutive failed authentication attempts (FIA_AFL.1/PIN)
    - The optional personal unblocking key (PUK.CH) can be used as PIN for the PIN authentication mechanism for the configuration TC-SCA-CL-Only for contact-based communication only.

  Note:

  1 PIN.CH may also be used as PIN with the PIN authentication mechanism. This is only possible for the configuration TC-SCA-CL-Only for contact-based communication. Using PIN.CH as PIN is beyond the scope of this ST.
- Symmetric Authentication Mechanism (FIA_UID.1.1(3), FIA_UAU.1.1(6), FIA_UAU.4.1/PACE(2), FIA_UAU.5.1/PACE(4) and FIA_UAU.5.2/PACE(2))
  - The cryptographic method for authenticity is CMAC (supplied by SF_HardwareCryptoLibrary) (FCS_COP.1/AES_MAC).
  - The method is configured to **delay the processing** of the authentication command after consecutive failed authentication attempts (FIA_AFL.1/AuthAdmin).

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

- Chip Authentication Protocol Version 1[186] according to [BSI-TR-03110-1-V220] (FIA_UAU.5/PACE)
  - The cryptographic method for confidentiality is AES/CBC (supplied by SF_HardwareCryptoLibrary) (FCS_COP.1/CA_ENC).
  - The cryptographic method for authenticity is CMAC (supplied by SF_HardwareCryptoLibrary) (FCS_COP.1/CA_MAC).
  - On error the user role is not identified/authenticated.
  - On success the session keys are created and stored for Secure Messaging (FCS_CKM.1/CA).
  - Keys and data in transient memory are overwritten after usage (FCS_CKM.4).
- Passive Authentication[187] for the verification of the authenticity of EF.CardSecurity (FIA_UAU.5/PACE)
  - EF.CardSecurity is signed by the SSCD-provisioning service provider allowing a PACE terminal to verify the authenticity of the TOE.
  - It contains the Chip Authentication Public Key which is used for identifying the SSCD.

The access control methods allow the execution of certain security relevant actions (e.g. self-tests) without successful user identification (FIA_UID.1) and authentication (FIA_UAU.1).

10.1.2.1 Administrator Identification and Authentication

Depending on the life cycle phase the administrator can gain access to the TOE in two different ways:

For the Life Cycle Phase “Usage/Preparation”:

The administrator is implicitly identified at the beginning of the Phase “Usage/Preparation” represented by the TOE life cycle phase MANUFACTURING. Before the administrator is able to start the TOE initialization, the command sequence received by the TOE software developer has to be performed, since the initial StartKey is not known to the administrator. The command sequence changes the secret StartKey (initial StartKey) to a default value ("default" in the sense of "the same value for each SSCD-provisioning service provider") which is known to the administrator. It is mandatory that the administrator change this default value to a value only known to him.

With this administrator-known (but otherwise secret) value for the StartKey, the TOE's life cycle can be switched from the MANUFACTURING to the ADMINISTRATION phase in order to carry out the TOE initialization and TOE personalization which comprises all the tasks performed by an SSCD-provisioning service provider during preparation of the TOE (see 4.4.3.2 Phase “Usage/Preparation”).

In order to separate the TOE initialization from the TOE personalization a re-authentication of the administrator is necessary. The TOE is switched from phase ADMINISTRATION to phase OPERATIONAL (permanently) after TOE initialization. The TOE personalization is secured by using the Symmetric Authentication Mechanism with the Administrator Personalization Key which is used to re-authenticate the administrator in order to allow the TOE to be switched back to phase ADMINISTRATION before the personalization tasks can be performed.

Note:

1. After the TOE has been (permanently) switched to phase OPERATIONAL it is only possible to switch it temporarily to phase ADMINISTRATION. In this sense ADMINISTRATION can be seen rather as a state than as a life cycle phase of the TOE. After a reset the TOE is always in phase OPERATIONAL.
2. The TOE initialization and TOE personalization may only take place in a trusted environment. (A.Env_Admin)

For the Life Cycle Phase “Usage/Operational”:

The administrator is identified and authenticated by using the PACE authentication method using the PIN.ADMIN as the shared password in the Phase “Usage/Operational” represented by the TOE life cycle phase OPERATIONAL.

Note:

1. By successfully authenticating himself using the PACE authentication method with PIN.ADMIN as the shared password the administrator sets the security attribute “SCD/SVD management” to “authorized” (FMT_SMF.1 and FMT_MSA.2).

[186] The Chip Authentication Protocol Version 1 is only applicable in cases where the communication between the TOE and another entity via trusted channel is mandatory.

[187] Passive Authentication is only applicable in cases where the communication between the TOE and another entity via trusted channel is mandatory.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

Before performing any management operations including the generation of the certificate thus including the SVD export from the TOE, the CGA or SSCD Issuing Application establishes the identity of the TOE as SSCD by

- reading and verifying EF.CardSecurity using Passive Authentication (FIA_UAU.5/PACE)
- using the Public Key from EF.CardSecurity together with Chip Authentication Protocol Version 1 to authenticate the SSCD (FIA_API.1).

SCD/SVD generation, SVD export from the TOE in this phase require an interaction with the SSCD-provisioning service provider or certification service provider (CSP) acting as administrator through a trusted channel established by the Chip Authentication Protocol Version 1 (FTP_ITC.1/SVD). (A.Env_Admin and A.CGA).

Additionally management operations, e.g. store certificate info to the SSCD in this phase also require an interaction with the SSCD-provisioning service provider acting as administrator through a trusted channel established by the Chip Authentication Protocol Version 1.

10.1.2.2 Signatory Identification and Authentication

Within the Phase "Usage/Operational" represented by the TOE life cycle phase OPERATIONAL the signatory is identified and authenticated either

- by using the transport PIN (PIN.T) either as the shared password with the PACE authentication method or as PIN with the PIN authentication mechanism on first usage upon receiving the TOE from the SSCD-provisioning service provider in order to disable the transport protection and activate (FMT_SMF.1)
  - the PIN for qualified signature (PIN.QES),
  - optionally the personal unblocking key (PUK.CH), if present and not already activated.

  Notes:

  1. The transport PIN (PIN.T) cannot be modified and can be used only once.
  2. The ability to activate the PIN of the Signatory (PIN.QES) is restricted to the signatory only after disabling the transport protection (FMT_MTD.1/RAD).
  3. If the transport PIN is not entered successfully or the transport PIN is blocked, the Signatory cannot be identified or authenticated.
  4. If the transport PIN is entered successfully, it is not possible to enter a transport PIN again.
  5. If the PIN of the Signatory (PIN.QES) is not set, it is not possible to enter the PIN of the Signatory (PIN.QES) successfully and it is not possible to block the PIN of the Signatory (PIN.QES) with unsuccessful consecutive authentication attempts.
  6. The transport PIN (PIN.T) must be used as shared password for the PACE authentication method for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.
  7. The transport PIN (PIN.T) can be used as shared password for the PACE authentication method **or** as PIN for the PIN authentication mechanism for the configuration TC-SCA-CL-Only for contact-based communication only.
- by using the optional personal unblocking key (PUK.CH) either as the shared password with the PACE authentication method in order to establish a trusted channel between the HID and the TOE for the management environment (FTP_ITC.1/VAD) or as PIN with the PIN authentication mechanism allowing
  - to unblock the PIN for qualified signature (PIN.QES). while ensuring the confidentiality and integrity of the **VAD** (FMT_MTD.1/Signatory).
  - to unblock the transport PIN (PIN.T) and the card holder PIN (PIN.CH) while ensuring the confidentiality and integrity of the **VAD**.
  - the modification of the personal unblocking key (PUK.CH) and the card holder PIN (PIN.CH) while ensuring the confidentiality and integrity of the **VAD**.

  Notes:

  1 PUK.CH must be used as shared password for the PACE authentication method for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only.

  2 PUK.CH can be used as shared password for the PACE authentication method **or** as PIN for the PIN authentication mechanism for the configuration TC-SCA-CL-Only for contact-based communication only.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

- by verifying the PIN for qualified signature (PIN.QES) with the PIN authentication mechanism in order to
  - create qualified electronic signatures,
  - modify the PIN for qualified signature (PIN.QES) itself (FMT_SMF.1 and FMT_MTD.1/Signatory),

  Note:

  1. By successfully authenticating himself using PIN verification with the PIN for qualified signature (PIN.QES) the signatory sets the security attribute “SCD operational” to “yes” (FMT_SMF.1 and FMT_MSA.2).

The TOE ensures re-authentication of the signatory for signature creation (FIA_UAU.6/Signature_Creation)

a) after each signature
if the personalization allows only a single signature,

b) after card reset or after Application QES was left or before the (N+1)-th signature in a row when limit for consecutive signatures is N
if the personalization allows a limited number of mass signatures in a row,

c) after card reset or after Application QES was left
if the personalization allows an unlimited number of mass signatures in a row.

10.1.2.3 PACE Terminal Identification and Authentication

Within the Phase “Usage/Operational” represented by the TOE life cycle phase OPERATIONAL the PACE Terminal is identified and authenticated by using the PACE authentication method using any of the available shared passwords (PIN.T, PIN.CH, optional PUK.CH, PIN.ADMIN and CAN) in order to establish a trusted channel between the HID and the TOE for both the signing and management environments or between the CGA or an issuer SSCD management application and the TOE for the management environment.

An identified and authenticated PACE Terminal is allowed to access EF.CardSecurity and exchange data with the TOE.

Depending on the shared password used with the PACE authentication method an additional user may be identified and authenticated and additional operations are allowed:

- by using the PACE authentication method using the transport PIN (PIN.T) as the shared password on first usage upon receiving the TOE from the SSCD-provisioning service provider in order to additionally identify and authenticate the Signatory and establish a trusted channel between the HID and the TOE for disabling the transport protection and activating the RAD (FTP_ITC.1/VAD and FMT_SMF.1).
- by using the PACE authentication method using the card holder PIN (PIN.CH) as the shared password in order to establish a trusted channel between the HID and the TOE for both the signing and management environments (FTP_ITC.1/VAD and FTP_ITC.1/DTBS) allowing
  - the verification of the PIN for qualified signature (PIN.QES) while ensuring the confidentiality and integrity of the **VAD**,
  - the creation of qualified electronic signatures[188] while ensuring the integrity of the **DTBS** respective **DTBS/R** (A.SCA),
  - the modification of the PIN for qualified signature (PIN.QES)[189] and the card holder PIN (PIN.CH) itself while ensuring the confidentiality and integrity of the **VAD** (FMT_SMF.1).

  Notes:

  1 Using PIN.CH as shared password used with the PACE authentication method only identifies and authenticates the PACE Terminal.

  2 For the TOE 'CardOS DI V5.4 QES Version 1.0' PIN.CH is only used as shared password for the PACE authentication method. However additional applications may use PIN.CH as PIN for the PIN authentication mechanism. This is only possible for the configuration TC-SCA-CL-Only for contact-based communication. Using PIN.CH as PIN is beyond the scope of this ST.
- by using the PACE authentication method using the optional personal unblocking key (PUK.CH) as the shared password in order to additionally identify and authenticate the Signatory and establish a trusted channel between the HID and the TOE for the management environment (FTP_ITC.1/VAD) allowing
  - to unblock the PIN for qualified signature (PIN.QES) while ensuring the confidentiality and integrity of the **VAD** (FMT_MTD.1/Signatory),

[188] Additionally requires verification of PIN.QES

[189] Additionally requires verification of PIN.QES

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

- to unblock the transport PIN (PIN.T) and the card holder PIN (PIN.CH) while ensuring the confidentiality and integrity of the **VAD**,
- the modification of the personal unblocking key (PUK.CH) and the card holder PIN (PIN.CH) while ensuring the confidentiality and integrity of the **VAD**.

- by using the PACE authentication method using the administrator PIN (PIN.ADMIN) as the shared password in order to to additionally identify and authenticate the Administrator and establish a trusted channel between the CGA or an issuer SSCD management application and the TOE for management environment (FTP_ITC.1/VAD and FTP_ITC.1/DTBS) allowing the execution of Chip Authentication Protocol Version 1.
- by using the PACE authentication method using the CAN as the shared password in order to establish a trusted channel between the HID and the TOE for both the signing and management environments (FTP_ITC.1/VAD and FTP_ITC.1/DTBS) allowing
  - the verification of the PIN for qualified signature (PIN.QES) while ensuring the confidentiality and integrity of the **VAD**,
  - the creation of qualified electronic signatures[190] while ensuring the integrity of the **DTBS** respective **DTBS/R** (A.SCA),
  - the modification of the PIN for qualified signature (PIN.QES)[191] while ensuring the confidentiality and integrity of the **VAD** (FMT_SMF.1),
  - to authenticate against PIN.CH, PUK.CH, PIN.T or PIN.ADMIN for the very last retry after setting the relevant password into a suspended state as protection against denial-of-service attacks.

  Note:

  1 The CAN is a non-blocking password with a minimum length of 6 digits that does not effectively represent a secret, but is restricted-revealable.

10.1.3 SF_AccessControl

This security function regulates all access by external entities to operations of the TOE which are only executed after the TSF allowed access. The security attributes used for this policy are stated in Table 9-1: Subjects and security attributes for access control. Generally, the access control policy is assigned to user roles. The identification, authentication and association of users to roles is realized by chapter 10.1.2 SF_UserIdentificationAuthentication.

This security functions also

- restricts the ability to read any keys or passwords (FMT_MTD.1/KEY_READ)
- denies any access not explicitly allowed

10.1.3.1 Access Control provided by the Signature_Creation_SFP

This aspect of the security function is responsible for the realization of the signature creation security function policy (Signature_Creation_SFP) and controls access to the signature creation functionality of the TOE.

The Signature_Creation_SFP is based on the security attribute “SCD operational” which is managed by

- FMT_MSA.1/Signatory
- FMT_MSA.2
- FMT_MSA.3

The TOE allows the creation of electronic signatures for **DTBS/R** with SCD if and only if (FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation, FDP_UIT.1/DTBS, FMT_MOF.1 and FMT_MSA.1/Signatory and FMT_MSA.2):

1. the transport protection is disabled
2. PACE authentication using PIN.CH or CAN as the shared password[192] has been successfully performed

[190] Additionally requires verification of PIN.QES

[191] Additionally requires verification of PIN.QES

[192] Applies only for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

3. the security attribute “SCD/SVD Management” is set to “not authorized” or “authorized”
4. the security attribute “SCD operational” is set to “yes”
5. the signature request is sent by an authorized signatory, see also chapter 10.1.2.2 Signatory Identification and Authentication
6. the signature request is sent in a manner protected from modification and insertion errors[193]

10.1.3.2 Access Control provided by the SCD/SVD_Generation_SFP

This aspect of the security function is responsible for the realization of the SCD/SVD pair generation security function policy (SCD/SVD_Generation_SFP) and controls access to the SCD/SVD pair generation functionality of the TOE.

The SCD/SVD_Generation_SFP is based on the security attribute “SCD/SVD Management” which is managed by

- FMT_MSA.1/Admin
- FMT_MSA.2
- FMT_MSA.3

Depending on the life cycle phase the TOE allows the generation of SCD/SVD pair either by the administrator alone or by the administrator together with the signatory:

For the Life Cycle Phase “Usage/Preparation”:

During the preparation of the TOE (see 4.4.3.2 Phase “Usage/Preparation”) the TOE allows the generation of SCD/SVD pair if and only if (FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FMT_MSA.1/Admin, FMT_MSA.2 and FMT_MSA.4):

1. the security attribute “SCD/SVD Management” is set to “authorized”
2. the security attribute “SCD operational” is set to “no”
3. the generation request is sent by an authorized administrator, see also chapter 10.1.2.1 Administrator Identification and Authentication

For the Life Cycle Phase “Usage/Operational”:

During the operation of the TOE (see 4.4.3.3 Phase “Usage/Operational”) the TOE allows the (re-)generation of SCD/SVD pair if and only if (FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FMT_MSA.1/Admin and FMT_MSA.2):

1. PACE authentication using PIN.ADMIN as the shared password has been successfully performed
2. Chip Authentication Protocol Version 1 has been successfully performed
3. the security attribute “SCD/SVD Management” is set to “authorized”
4. the security attribute “SCD operational” is set to “yes”
5. the generation request is sent by an authorized administrator, see also chapter 10.1.2.1 Administrator Identification and Authentication **and** authorized signatory, see also chapter 10.1.2.2 Signatory Identification and Authentication

10.1.3.3 Access Control provided by the SVD_Transfer_SFP

This aspect of the security function is responsible for the realization of the SVD transfer security function policy (SVD_Transfer_SFP) and controls access to the SVD export functionality of the TOE.

The TOE allows the export of the SVD if and only if (FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer):

1. PACE authentication using PIN.ADMIN as the shared password has been successfully performed
2. Chip Authentication Protocol Version 1 has been successfully performed
3. the export request is sent by an authorized administrator, see also chapter 10.1.2.1 Administrator Identification and Authentication
4. the exported SVD is sent in a manner to provide the CGA with the ability to verify evidence of the validity of the SVD (FDP_DAU.2/SVD).

[193] Applies only for the configuration TC-SCA-Mandatory for all communication interfaces and for the configuration TC-SCA-CL-Only for contactless communication only

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

Note:

1. Chip Authentication Protocol Version 1 shall be used in order to provide the CGA with the ability to verify the identity of the SSCD.

10.1.3.4 Access Control provided by the Access_Control_SFP

This aspect of the security function is responsible for the realization of the access control security function policy (Access_Control_SFP) and controls

- access to EF.CardSecurity of the TOE and
- data exchange with the TOE.

The TOE allows the access to EF.CardSecurity and data exchange with the TOE if and only if (FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_UCT.1/TRM and FDP_UIT.1/TRM):

1. the access request is sent by an authorized PACE Terminal, see also chapter 10.1.2.3 PACE Terminal Identification and Authentication
2. the access request is sent in a manner protected from unauthorized disclosure, modification, deletion, insertion and replay errors

10.1.4 SF_KeyManagement

This security function is responsible for the management of

- the SCD/SVD pair which is used by the signatory to create electronic signatures. This includes the correct generation and the termination of the SCD/SVD pair.
- the Chip Authentication Private Key which is used during Chip Authentication Protocol Version 1 in order to prove the identity of the SSCD.

The TOE supports onboard generation (supplied by SF_HardwareCryptoLibrary) of

a) EC signature key pairs with a key length of 256, 384, 512 or 521 bits (FCS_CKM.1/EC) and

b) RSA signature key pairs with a key length of 2048 or 3072 bits (FCS_CKM.1/RSA).

The generation is done with secure values for SCD/SVD parameters so that the key pairs fulfill the corresponding requirements of the standards as listed in [Infineon-ST-M7892-D11-G12] and for

- EC key pairs [ANSI-X9.62], [ISO-IEC-14888-3] and [IEEE-1363] (FCS_CKM.1/EC)
- RSA key pairs [RSA-PKCS1-v2.2] and [IEEE-1363] (FCS_CKM.1/RSA).

The TOE uses a hybrid deterministic random number generator for the generation of the SCD/SVD pair. The generation is furthermore protected against electromagnetic emanation, simple power analysis (SPA) and timing attacks, see also chapter 10.1.6 SF_Protection below.

In the case that a signature key pair is terminated on request of the signatory, the signature key pair will be deleted by the TOE (FCS_CKM.4).

The SCD is identified by security attribute "SCD identifier". The security attribute "SCD identifier" may have arbitrary values. The Administrator can set/change security attribute "SCD identifier" to a desired value (FMT_SMF.1). The Administrator is thus able to override the default values when an object or information (here: SCD) is created (FMT_MSA.3).

Only during the preparation of the TOE (see 4.4.3.2 Phase “Usage/Preparation”) the TOE allows to load the Chip Authentication Private Key if and only if the import request is sent by an authorized administrator, see also chapter 10.1.2.1 Administrator Identification and Authentication (FMT_MTD.1/CAPK).

10.1.5 SF_SignatureCreation

This security function is responsible for signature creation using the SCD of the signatory. Before a signature is created by the TOE, the signatory has to be authenticated successfully, see also chapter 10.1.2.2 Signatory Identification and Authentication.

Depending on its configuration the TOE allows to create **single** or **mass** signatures[194].

[194] Mass signature generation is used to create either a limited or unlimited number of electronic signatures in a row for an automated process.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Note:

1. Mass signatures are allowed only in a trusted environment (A.Env_Mass_Signature).

10.1.5.1 Signature Creation with EC

This aspect of the security function creates EC signatures (FCS_COP.1/EC) for hash values using the SCD of the signatory. The signatures created meet the following standards:

- section 7.3 in [ANSI-X9.62],
- section 6.4.3 in [ISO-IEC-14888-3] and
- section 7.2.7 in [IEEE-1363], see [Infineon-ST-M7892-D11-G12], 7.1.4.7 Elliptic Curve DSA (ECDSA) Signature Generation and Verification

because this TOE uses the EC crypto library of the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12), supplied by SF_HardwareCryptoLibrary.

The security function supports EC key lengths of 256 - 521 bits using curves (FCS_COP.1/EC)

1. for 256 bits:
   a) P-256 ([NIST-FIPS-186-4], chapter D.2.3 "Curve P-256", aka secp256r1)
   b) brainpoolP256r1 ([RFC-5639-2010-03], chapter 3.4)
2. for 384 bits:
   a) P-384 ([NIST-FIPS-186-4], chapter D.2.4 "Curve P-384", aka secp384r1)
   b) brainpoolP384r1 ([RFC-5639-2010-03], chapter 3.6)
3. for 512 bits:

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

   P-256 ([NIST-FIPS-186-4], chapter D.2.5 "Curve P-521", aka secp521r1).

10.1.5.2 Signature Creation with RSA

This aspect of the security function creates RSA signatures (FCS_COP.1/RSA) for hash values with PKCS1 block type 1 or PSS padding using the SCD of the signatory. The signatures created meet the following standards:

- section 5.2.1 RSASP1 in [RSA-PKCS1-v2.2] and
- section 8.2.4 in [IEEE-1363], see [Infineon-ST-M7892-D11-G12], 7.1.4.4 Rivest-Shamir-Adleman (RSA) operation

because this TOE uses the RSA crypto library of the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12), supplied by SF_HardwareCryptoLibrary. The padding is done according to RSASSA-PSS and RSASSA-PKCS1-v1_5.

The security function supports RSA key lengths of 2048 and 3072 bits (FCS_COP.1/RSA).

10.1.5.3 TOE IT environment generated hash values

The hash value used for the signature creation is calculated over the DTBS in the TOE IT environment and sent to the TOE under the control of the Signature_Creation_SFP, see 10.1.3.1 Access Control provided by the Signature_Creation_SFP.

For the signature creation functionality see 10.1.5 SF_SignatureCreation.

10.1.5.4 TOE generated hash values

In case that DTBS instead of a hash value (DTBS/R) is sent to the TOE under the control of the Signature_Creation_SFP, see 10.1.3.1 Access Control provided by the Signature_Creation_SFP, the TOE directly generates a hash value (FCS_COP.1/SHA) over the sent DTBS first which is used afterward for the signature creation.

For the signature creation functionality see 10.1.5 SF_SignatureCreation.

Note:

1. This TOE uses SHA-224 and SHA-384 which are both provided by CardOS DI V5.4.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

10.1.5.5 Hash last round

In case that the hash value (DTBS/R) is only partly computed in the IT environment an intermediate hash value with the remainder of DTBS is sent to the TOE under the control of the Signature_Creation_SFP, see 10.1.3.1 Access Control provided by the Signature_Creation_SFP. The TOE first computes the 'last round(s)' over the remainder of DTBS and the intermediate hash value (FCS_COP.1/SHA). The final hash value is used afterward for the signature creation.

For the signature creation functionality see 10.1.5 SF_SignatureCreation.

Note:

1. This TOE uses SHA-224 and SHA-384 which are both provided by CardOS DI V5.4.
2. Last round hash values may be used if a signature for large data shall be generated as the IT environment is able to hash much faster than the card.

10.1.6 SF_Protection

This security function is responsible for the protection of the TSF, TSF data and user data. The TOE runs a suite of tests to demonstrate the correct operation of the security assumptions provided by the IC platform that underlies the TSF. The following tests are performed during initial start-up:

- The SLE78CLFX*P* (M7892 Design Steps D11 and G12) provides a high security initialization software concept. The self-test software (STS) is activated by the chip after a cold or warm reset (ISO-reset with I/O=1). It contains diagnostic routines for the chip, see [Infineon–Chip-HW-Ref-M7892].
- After erasure of RAM the state of the User EEPROM is tested and, if not yet initialized, this will be done.
- The User EEPROM heap is checked for consistency. If it is not valid, the TOE will preserve a secure state (TOE life cycle phase DEATH).
- The backup buffer is checked and its data is restored to User EEPROM, if they were saved because of a command interruption.
- The integrity of stored TSF executable code is verified. If this check fails, the TOE will preserve a secure state (TOE life cycle phase DEATH).
- The integrity of stored data (objects and files) is verified before their use.
- The hardware sensors, the symmetric coprocessor and the random number generator are tested. If one of the tests fails, the chip platform will perform a security reset.

The TOE will furthermore run tests during the generation of the SCD/SVD pair (10.1.4 SF_KeyManagement) and during signature creation (10.1.5SF_SignatureCreation) (FPT_TST.1).

The signature creation process is implemented in a way which does not disclose the SCD by

1) measuring the shape and amplitude of signals or
2) signals on the electromagnetic field, power consumption, clock, or I/O lines or
3) during internal operations or data transmissions

in order to find the time between events of the TOE during the signature calculation. It is furthermore not possible to gain unauthorized access to the SCD using the TOE's contactless/contact interface and circuit contacts (FPT_EMS.1/SSCD). For tests during signature creation the code of the Infineon Crypto Library (RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010) is used. The certificate [BSI-DSZ-CC-0891] of the chip SLE78CLFX*P* (M7892 Design Steps D11 and G12) (Common Criteria level EAL 6+) cover the functionality for signature creation.

The correct generation of the SCD/SVD pair is demonstrated by performing the following checks:

- The TOE's life cycle phase is checked. The SCD/SVD pair generation can only be done either by the administrator alone or by the administrator together with the signatory.
- Before a random number from the PTRNG is used as random source for the hybrid deterministic random number generator the correct functioning of the random number generator is checked by reading out the status register of PTRNG.
- All command parameters are checked for consistency.
- Access rights are checked.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

If a critical failure occurs during these tests, the TOE will preserve a secure state (FPT_FLS.1). This comprises the following types of failures:

- Failure of sensors
- Failure of Active Shield
- Failure of cryptographic operation, e.g. during signature creation
- Memory failures during TOE execution
- Out of range failures of temperature, clock and voltage sensors
- Failures during random number generation

After the generation of the SCD/SVD pair no information of used resources is available (FDP.RIP.1).

The TOE will also run tests before command execution for VAD verification, RAD modification and RAD unblocking (FPT_TST.1). These processes are implemented in a way which does not disclose the RAD by

1) measuring the shape and amplitude of signals or
2) signals on the electromagnetic field, power consumption, clock, or I/O lines or
3) during internal operations or data transmissions

in order to find the time between events of the TOE during the signature calculation. It is furthermore not possible to gain unauthorized access to the RAD using the TOE's contactless/contact interface and circuit contacts (FPT_EMS.1/SSCD).

The TOE is furthermore able to detect physical or mechanical tampering attempts (FPT_PHP.1). This comprises tampering attempts before start-up and during operation. If the underlying IC hardware is attacked by physical or mechanical means, the TOE will respond automatically in form of a continuously generated reset and the TOE functionality will be blocked (FPT_PHP.3).

This security function actively destroys temporarily stored SCD, VAD and RAD immediately after their use – as soon as these data are dispensable (FDP_RIP.1).

The PACE authentication method and Chip Authentication Protocol Version 1 are implemented in a way which does not disclose the

1. PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}),
2. the ephemeral private key ephem-SK_{PICC}-PACE,
3. Chip Authentication private key
4. Chip Authentication session keys (CA-K_{MAC}, CA-K_{Enc})

by

1) measuring the shape and amplitude of signals or
2) signals on the electromagnetic field, power consumption, clock, or I/O lines or
3) during internal operations or data transmissions

in order to find the time between events of the TOE during the signature calculation. It is furthermore not possible to gain unauthorized access to the

1. PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}),
2. the ephemeral private key ephem-SK_{PICC}-PACE,
3. Chip Authentication private key
4. Chip Authentication session keys (CA-K_{MAC}, CA-K_{Enc})

using the TOE's contactless/contact interface and circuit contacts (FPT_EMS.1/KEYS).

The following data persistently stored by TOE has the user data attribute "integrity checked persistent stored data" (FDP_RIP.1):

- SCD
- SVD

Also the DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data" (FDP_RIP.1).

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

If the integrity of SCD, SVD or DTBS/R is violated, the TOE will prohibit the usage of the altered data and inform the signatory about the integrity error by means of an error code (FDP_SDI.2/Persistent and FDP_SDI.2/DTBS).

The TOE protects itself against interference and logical tampering by the following measures:

Each application removes its own data from the used memory area at the latest after execution of a command.

- Clearance of sensitive data, as soon as possible (when they are dispensable)
- Encapsulation of context data (security relevant status variables, etc.)
- Use of the chips MMU (Memory Management Unit)
- Separation of User ROM and Test ROM, where the chip's self-test software is located, and to which entries are not possible (apart from cold or warm reset)

The TOE protects itself against bypass by not allowing any function in the TSF to proceed if a prior security enforcement function was not executed successfully. The TOE always checks that the appropriate user is successfully authenticated (cf. 10.1.2 SF_UserIdentificationAuthentication) for a certain action.

The following table shows the coverage of the SFRs by TSFs.

SFR	TSFs
FCS_CKM.1/EC	SF_HardwareCryptoLibrary, SF_KeyManagement
FCS_CKM.1/RSA	SF_HardwareCryptoLibrary, SF_KeyManagement
FCS_CKM.1/DH_PACE	SF_HardwareCryptoLibrary, SF_UserIdentificationAuthentication
FCS_CKM.1/CA	SF_HardwareCryptoLibrary, SF_UserIdentificationAuthentication
FCS_CKM.4	SF_UserIdentificationAuthentication, SF_KeyManagement
FCS_COP.1/EC	SF_HardwareCryptoLibrary, SF_SignatureCreation
FCS_COP.1/RSA	SF_HardwareCryptoLibrary, SF_SignatureCreation
FCS_COP.1/SHA	SF_HardwareCryptoLibrary, SF_SignatureCreation
FCS_COP.1/PACE_ENC	SF_HardwareCryptoLibrary, SF_UserIdentificationAuthentication
FCS_COP.1/PACE_MAC	SF_HardwareCryptoLibrary, SF_UserIdentificationAuthentication
FCS_COP.1/CA_ENC	SF_HardwareCryptoLibrary, SF_UserIdentificationAuthentication
FCS_COP.1/CA_MAC	SF_HardwareCryptoLibrary, SF_UserIdentificationAuthentication
FCS_COP.1/AES_MAC	SF_HardwareCryptoLibrary, SF_UserIdentificationAuthentication
FCS_RNG.1	SF_HardwareCryptoLibrary, SF_UserIdentificationAuthentication
FDP_ACC.1/TRM	SF_AccessControl
FDP_ACF.1/TRM	SF_AccessControl
FDP_ACC.1/SCD/SVD_Generation	SF_AccessControl
FDP_ACF.1/SCD/SVD_Generation	SF_AccessControl
FDP_ACC.1/SVD_Transfer	SF_AccessControl
FDP_ACF.1/SVD_Transfer	SF_AccessControl
FDP_ACC.1/Signature_Creation	SF_AccessControl
FDP_ACF.1/Signature_Creation	SF_AccessControl
FDP_UCT.1/TRM	SF_AccessControl
FDP_UIT.1/TRM	SF_AccessControl
FDP_UIT.1/DTBS	SF_AccessControl
FDP_RIP.1	SF_Protection
FDP_SDI.2/Persistent	SF_Protection
FDP_SDI.2/DTBS	SF_Protection
FDP_DAU.2/SVD	SF_AccessControl
FIA_UID.1	SF_UserIdentificationAuthentication
FIA_UAU.1	SF_UserIdentificationAuthentication
FIA_UAU.4/PACE	SF_UserIdentificationAuthentication
FIA_UAU.5/PACE	SF_UserIdentificationAuthentication
FIA_UAU.6/PACE	SF_UserIdentificationAuthentication
FIA_UAU.6/CA	SF_UserIdentificationAuthentication
FIA_UAU.6/Signature_Creation	SF_UserIdentificationAuthentication
FIA_AFL.1/RAD	SF_UserIdentificationAuthentication
FIA_AFL.1/PIN	SF_UserIdentificationAuthentication
FIA_AFL.1/PACE	SF_UserIdentificationAuthentication
FIA_AFL.1/Suspend_PIN	SF_UserIdentificationAuthentication

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

SFR	TSFs
FIA_AFL.1/Block_PIN	SF_UserIdentificationAuthentication
FIA_AFL.1/AuthAdmin	SF_UserIdentificationAuthentication
FIA_API.1	SF_UserIdentificationAuthentication
FMT_SMR.1	SF_UserIdentificationAuthentication
FMT_SMF.1	SF_UserIdentificationAuthentication, SF_KeyManagement
FMT_MOF.1	SF_AccessControl
FMT_MSA.1/Admin	SF_AccessControl
FMT_MSA.1/Signatory	SF_AccessControl
FMT_MSA.2	SF_UserIdentificationAuthentication, SF_AccessControl
FMT_MSA.3	SF_AccessControl, SF_KeyManagement
FMT_MSA.4	SF_AccessControl
FMT_MTD.1/RAD	SF_UserIdentificationAuthentication
FMT_MTD.1/Signatory	SF_UserIdentificationAuthentication
FMT_MTD.1/KEY_READ	SF_AccessControl
FMT_MTD.1/CAPK	SF_KeyManagement
FPT_EMS.1/SSCD	SF_HardwareCryptoLibrary, SF_Protection
FPT_EMS.1/KEYS	SF_HardwareCryptoLibrary, SF_Protection
FPT_FLS.1	SF_HardwareCryptoLibrary, SF_Protection
FPT_PHP.1	SF_HardwareCryptoLibrary, SF_Protection
FPT_PHP.3	SF_HardwareCryptoLibrary, SF_Protection
FPT_TST.1	SF_HardwareCryptoLibrary, SF_Protection
FTP_ITC.1/SVD	SF_UserIdentificationAuthentication
FTP_ITC.1/VAD	SF_UserIdentificationAuthentication
FTP_ITC.1/DTBS	SF_UserIdentificationAuthentication

Table 10-1: Coverage of SFRs for the TOE by TSFs

10.2 Statement of Compatibility

This is a statement of compatibility between this composite security target (Composite-ST) and the platform security target (Platform-ST) of the chip SLE78CLFX*P* (M7892 Design Steps D11 and G12) [Infineon-ST-M7892-D11-G12].

10.2.1 Classification of Platform TSFs

The following table shows the relevance of the platform TSFs for the Composite-ST.

Platform TSFs	Relevant	Not relevant
SF_DPM: Device Phase Management	x	
SF_PS: Protection against Snooping	x	
SF_PMA: Protection against Modification Attacks	x	
SF_PLA: Protection against Logical Attacks	x	
SF_CS: Cryptographic Support	x	
SF_MAE: Mutual Authentication Extension		x

Table 10-2: Classification of Platform-TSFs

10.2.2 Compatibility: TOE Security Environment

10.2.2.1 Threats

The threats of the TOE and the platform can be mapped or are not relevant. They show no conflicts between each other.

- Threats of the TOE
  - T.SCD_Divulg (Storing, copying and releasing of the signature creation data): matches T.Leak-Inherent, T.Leak-Forced and T.RND of the Platform-ST

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

- T.SCD_Derive (Derive the signature creation data): no conflict
- T.Hack_Phys (Physical attacks through the TOE interfaces): matches T.Phys-Probing, T.Phys-Manipulation, T.Malfunction and T.Abuse-Func of the Platform-ST
- T.SVD_Forgery (Forgery of the signature verification data): no conflict
- T.SigF_Misuse (Misuse of the signature creation function of the TOE): no conflict
- T.DTBS_Forgery (Forgery of the DTBS/R): no conflict
- T.Sig_Forgery (Forgery of the electronic signature): no conflict
- T.Skimming (Skimming SSCD / Capturing Card-Terminal Communication): no conflict
- T.Eavesdropping (Eavesdropping on the communication between the TOE and the PACE terminal): no conflict

- Threats of the platform
  - T.Leak-Inherent (Inherent Information Leakage): matches T.SCD_Divulg of the TOE ST
  - T.Phys-Probing (Physical Probing): matches T.Hack_Phys of the TOE ST
  - T.Malfunction (Malfunction due to Environmental Stress): matches T.Hack_Phys of the TOE ST
  - T.Phys-Manipulation (Physical Manipulation): matches T.Hack_Phys of the TOE ST
  - T.Leak-Forced (Forced Information Leakage): matches T.SCD_Divulg of the TOE ST
  - T.Abuse-Func (Abuse of Functionality): matches T.Hack_Phys of the TOE ST
  - T.RND (Deficiency of Random Numbers): matches T.SCD_Divulg of the TOE ST

	T.SCD_Divulg	T.Hack_Phys
T.Leak-Inherent	x	
T.Phys-Probing		x
T.Malfunction		x
T.Phys-Manipulation		x
T.Leak-Forced	x	
T.Abuse-Func		x
T.RND	x	

10.2.2.2 Organizational Security Policies

The organizational security policies of the TOE and the platform have no conflicts between each other. They are shown in the following list.

- Organizational security policies of the TOE
  - P.CSP_QCert (Qualified certificate): no conflict
  - P.QSign (Qualified electronic signatures): no conflict
  - P.Sigy_SSCD (TOE as secure signature creation device): no conflict
  - P.Sig_Non-Repud (Non-repudiation of signatures): no conflict
- Organizational security policies of the platform
  - P.Process-TOE (Identification during TOE Development and Production): no conflict
  - P.Crypto-Service (Cryptographic services of the TOE): no conflict
  - P.Lim_Block_Loader (Limiting and Blocking the Loader Functionality): no conflict
  - P.Add-Functions (Additional Specific Security Functionality): no conflict

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

10.2.2.3 Assumptions

The following list shows that neither assumptions of the TOE nor of the platform have any conflicts between each other. They are either not relevant for this ST or are covered by appropriate security objectives.

- Assumptions of the TOE
  - A.CGA (Trustworthy certification generation application): no conflict
  - A.SCA (Trustworthy signature creation application): no conflict
  - A.Env_Admin (Environment for administrator): no conflict
  - A.Env_Mass_Signature (Environment for a mass signature TOE): no conflict
- Assumptions of the hardware
  - A.Process-Sec-IC (Protection during Packaging, Finishing and Personalization): no conflict
  - A.Resp-Appl (Treatment of User data of the Composite TOE): All Security Objectives of this Composite TOE aim to protect the user data, especially SCD, SVD, DTBS and RAD
  - A.Key-Function (Usage of Key-dependent Functions): OT.EMSEC_Design requires that Key-dependent functions are implemented in a way that they are not susceptible to leakage attacks

The following table shows the relevance of the assumptions from the platform for the Composite-ST.

Platform Assumptions	Relevant	Not relevant
A.Process-Sec-IC: Protection during Packaging, Finishing and Personalization		x
A.Resp-Appl: Treatment of User data of the Composite TOE	x	
A.Key-Function: Usage of Key-dependent Functions	x	

Table 10-3: Classification of Platform-Assumptions

10.2.2.4 Security Objectives

Some of the security objectives of the TOE and the platform can be mapped directly. None of them show any conflicts between each other.

- Security objectives for the TOE
  - OT.Lifecycle_Security (Life cycle security): no conflicts
  - OT.SCD/SVD_Auth_Gen (Authorized SCD/SVD generation): no conflicts
  - OT.SCD_Unique (Uniqueness of the signature creation data): covered by O.Add-Functions of the Platform-ST
  - OT.SCD_SVD_Corresp (Correspondence between SVD and SCD): covered by O.Add-Functions of the Platform-ST
  - OT.SCD_Secrecy (Secrecy of the signature creation data): covered by O.Leak-Forced and O.Add-Functions of the Platform-ST
  - OT.Sig_Secure (Cryptographic security of the electronic signature): covered by O.Add-Functions of the Platform-ST
  - OT.Sigy_SigF (Signature creation function for the legitimate signatory only): no conflicts
  - OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE): no conflicts
  - OT.EMSEC_Design (Provide physical emanations security): covered by O.Leak-Inherent of the Platform-ST
  - OT.Tamper_ID (Tamper detection): covered by O.Phys-Probing, O.Malfunction and O.Phys-Manipulation of the Platform-ST
  - OT.Tamper_Resistance (Tamper resistance): covered by O.Phys-Probing, O.Malfunction and O.Phys-Manipulation of the Platform-ST
  - OT.TOE_SSCD_Auth (Authentication proof as SSCD): no conflicts
  - OT.TOE_TC_SVD_Exp (TOE trusted channel for SVD export): no conflicts
  - OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import): no conflicts

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

- OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS import): no conflicts

- Security objectives for the operational environment: no conflict for any of the security objectives with those of the platform
- Security objectives for the platform

  - O.Phys-Manipulation (Protection against Physical Manipulation): covered by OT.Tamper_ID and OT.Tamper_Resistance of the TOE ST
  - O.Phys-Probing (Protection against Physical Probing): covered by OT.Tamper_ID and OT.Tamper_Resistance of the TOE ST
  - O.Malfunction (Protection against Malfunction): covered by OT.Tamper_ID and OT.Tamper_Resistance of the TOE ST
  - O.Leak-Inherent (Protection against Inherent Information Leakage): covered by OT.EMSEC_Design of the TOE ST
  - O.Leak-Forced (Protection against Forced Information Leakage): covered by OT.SCD_Secrecy of the TOE ST
  - O.Abuse-Func (Protection against Abuse of Functionality): no conflict
  - O.Identification (TOE Identification): no conflict
  - O.RND (Random Numbers): basic objective for the security of the TOE; no conflicts
  - O.Cap_Avail_Loader (Capability and availability of the Loader): no conflicts
  - O.TDES (Cryptographic service Triple-DES): no conflicts
  - O.AES (Cryptographic service AES): no conflicts
  - O.SHA (Cryptographic service Hash function): no conflicts
  - O.Authentication (Authentication to external entities): no conflicts
  - O.Prot_TSF_Confidentiality (Protection of the confidentiality of the TSF): no conflicts
  - O.Ctrl_Auth_Loader/Package1+ (Access control and authenticity for the Loader): no conflicts
  - O.Add-Functions (Additional Specific Security Functionality): covered by OT.SCD_Unique, OT.SCD_SVD_Corresp, OT.SCD_Secrecy and OT.Sig_Secure of the TOE ST
  - O.Mem-Access (Area based Memory Access Control): no conflicts
  - OE.Lim_Block_Loader (Limitation of capability and blocking the Loader): no conflicts
  - OE.Loader_Usage/Package1+ (Secure usage of the Loader): no conflicts
  - OE.TOE_Auth (External entities authenticating of the TOE): no conflicts
  - OE.Resp-Appl (Treatment of user data of the Composite TOE): no conflicts
  - OE.Process-Sec-IC (Protection during composite product manufacturing): no conflicts

The following table shows the mapping of the security objectives of the platform to those of the Composite-ST (including those of the environment). Only the security objectives that can be mapped directly are shown.

	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
O.Phys-Manipulation						x	x

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

O.Phys-Probing						x	x
O.Malfunction						x	x
O.Leak-Inherent					x		
O.Leak-Forced			x				
O.Add-Functions	x	x	x	x			

Table 10-4: Mapping of security objectives of the platform to TOE security objectives

10.2.2.5 Security Requirements

The relevant security requirements of the TOE and the platform can be mapped directly. None of them show any conflicts between each other.

- Security requirements of the TOE
  - FCS_CKM.1/EC (Cryptographic key generation – EC): matches FCS_CKM.1/EC of the Platform-ST
  - FCS_CKM.1/RSA (Cryptographic key generation – RSA): matches FCS_CKM.1/RSA of the Platform-ST
  - FCS_CKM.1/DH_PACE (Cryptographic key generation – Diffie-Hellman for PACE session keys): matches FCS_COP.1/ECDH of the Platform-ST
  - FCS_CKM.1/CA (Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys): matches FCS_COP.1/ECDH of the Platform-ST
  - FCS_CKM.4 (Cryptographic key destruction): no conflicts
  - FCS_COP.1/EC (Cryptographic operation – EC): matches FCS_COP.1/ECDSA of the Platform-ST
  - FCS_COP.1/RSA (Cryptographic operation – RSA): matches FCS_COP.1/RSA of the Platform-ST
  - FCS_COP.1/SHA (Cryptographic operation – Hash calculation): matches FCS_COP.1/SHA of the Platform-ST
  - FCS_COP.1/PACE_ENC (Cryptographic operation – Encryption / Decryption AES): matches FCS_COP.1/ AES_SCL of the Platform-ST
  - FCS_COP.1/PACE_MAC (Cryptographic operation – MAC): matches FCS_COP.1/ AES_SCL of the Platform-ST
  - FCS_COP.1/CA_ENC (Cryptographic operation – Symmetric Encryption / Decryption AES): matches FCS_COP.1/ AES_SCL of the Platform-ST
  - FCS_COP.1/CA_MAC (Cryptographic operation – MAC): matches FCS_COP.1/ AES_SCL of the Platform-ST
  - FCS_COP.1/AES_MAC (Cryptographic operation – MACing with AES): matches FCS_COP.1/ AES_SCL of the Platform-ST
  - FCS_RNG.1 (Random number generation): matches FCS_RNG.1 of the Platform-ST
  - FDP_ACC.1/TRM (Subset access control – Terminal Access): matches FDP_ACC.1 of the Platform-ST
  - FDP_ACF.1/TRM (Security attribute based access control – Terminal Access): matches FDP_ACF.1 of the Platform-ST
  - FDP_ACC.1/SCD/SVD_Generation (Subset access control): matches FDP_ACC.1 of the Platform-ST
  - FDP_ACF.1/SCD/SVD_Generation (Security attribute based access control): matches FDP_ACF.1 of the Platform-ST
  - FDP_ACC.1/SVD_Transfer (Subset access control): matches FDP_ACC.1 of the Platform-ST
  - FDP_ACF.1/SVD_Transfer (Subset access control): matches FDP_ACF.1 of the Platform-ST
  - FDP_ACC.1/Signature_Creation (Subset access control): matches FDP_ACC.1 of the Platform-ST
  - FDP_ACF.1/Signature_Creation (Security attribute based access control): matches FDP_ACF.1 of the Platform-ST
  - FDP_UCT.1/TRM (Basic data exchange confidentiality – Terminal): no conflicts

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

- FDP_UIT.1/TRM (Data exchange integrity – Terminal): no conflicts
- FDP_UIT.1/DTBS (Data exchange integrity – DTBS): no conflicts
- FDP_RIP.1 (Subset residual information protection): no conflicts
- FDP_SDI.2/Persistent (Stored data integrity monitoring and action): no conflicts
- FDP_SDI.2/DTBS (Stored data integrity monitoring and action): no conflicts
- FDP_DAU.2/SVD (Data Authentication with Identity of Guarantor): no conflicts
- FIA_UID.1 (Timing of identification): no conflicts
- FIA_UAU.1 (Timing of authentication): no conflicts
- FIA_UAU.4/PACE (Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE): no conflicts
- FIA_UAU.5/PACE (Multiple authentication mechanisms): no conflicts
- FIA_UAU.6/PACE (Re-authenticating of Terminal by the TOE): no conflicts
- FIA_UAU.6/CA (Re-authenticating – Re-authenticating of Terminal by the TOE): no conflicts
- FIA_UAU.6/Signature_Creation (Re-authenticating for Signature Creation): no conflicts
- FIA_AFL.1/RAD (Authentication failure handling – for Signatory PIN): no conflicts
- FIA_AFL.1/PIN (Authentication failure handling – for PINs other than the Signatory PIN): no conflicts
- FIA_AFL.1/PACE (Authentication failure handling – PACE authentication using non-blocking authorization data): no conflicts
- FIA_AFL.1/Suspend_PIN (Authentication failure handling – Suspending PIN): no conflicts
- FIA_AFL.1/Block_PIN (Authentication failure handling – Blocking PIN): no conflicts
- FIA_AFL.1/AuthAdmin (Authentication failure handling – of administrator for personalization): no conflicts
- FIA_API.1 (Authentication proof of identity): no conflicts
- FMT_SMR.1 (Security roles): no conflicts
- FMT_SMF.1 (Security management functions): no conflicts
- FMT_MOF.1 (Management of security functions behavior): no conflicts
- FMT_MSA.1/Admin (Management of security attributes): no conflicts
- FMT_MSA.1/Signatory (Management of security attributes): no conflicts
- FMT_MSA.2 (Secure security attributes): no conflicts
- FMT_MSA.3 (Static attribute initialization): no conflicts
- FMT_MSA.4 (Security attribute value inheritance): no conflicts
- FMT_MTD.1/RAD (Management of TSF data): no conflicts
- FMT_MTD.1/Signatory (Management of TSF data): no conflicts
- FMT_MTD.1/KEY_READ (Management of TSF data): no conflicts
- FMT_MTD.1/CAPK (Management of TSF data - Chip Authentication Private Key): no conflicts
- FPT_EMS.1/SSCD (TOE Emanation of SCD and RAD): matches FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1 of the Platform-ST
- FPT_EMS.1/KEYS (TOE Emanation of secret/private keys): matches FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1 of the Platform-ST
- FPT_FLS.1 (Failure with preservation of secure state): matches FRU_FLT.2 and FPT_FLS.1 of the Platform-ST
- FPT_PHP.1 (Passive detection of physical attack): matches FRU_FLT.2, FPT_FLS.1 and FPT_PHP.3 of the Platform-ST

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

  - FPT_PHP.3 (Resistance to physical attack): matches FRU_FLT.2, FPT_FLS.1 and FPT_PHP.3 of the Platform-ST
  - FPT_TST.1 (TSF testing): matches FRU_FLT.2 and FPT_TST.2 of the Platform-ST
  - FTP_ITC.1/SVD (Inter-TSF trusted channel): no conflicts
  - FTP_ITC.1/VAD (Inter-TSF trusted channel – TC Human Interface Device): no conflicts
  - FTP_ITC.1/DTBS (Inter-TSF trusted channel – Signature creation Application): no conflicts
- Security requirements of the platform
  - FRU_FLT.2 (Limited fault tolerance): covered by FPT_FLS.1, FPT_PHP.1, FPT_PHP.3 and FPT_TST.1 of the TOE ST
  - FPT_FLS.1 (Failure with preservation of secure state): covered by FPT_FLS.1, FPT_PHP.1 and FPT_PHP.3 of the TOE ST
  - FMT_LIM.1 (Limited capabilities): no conflicts
  - FMT_LIM.2 (Limited availability): no conflicts
  - FAU_SAS.1 (Audit storage): no conflicts
  - FDP_SDC.1 (Stored data confidentiality): no conflicts
  - FDP_SDI.2 (Stored data integrity monitoring and action): no conflicts
  - FPT_PHP.3 (Resistance to physical attack): covered by FPT_PHP.1 and FPT_PHP.3 of the TOE ST
  - FDP_ITT.1 (Basic internal transfer protection): covered by FPT_EMS.1/* of the TOE ST
  - FPT_ITT.1 (Basic internal TSF data transfer protection): covered by FPT_EMS.1/* of the TOE ST
  - FDP_IFC.1 (Subset information flow control): covered by FPT_EMS.1/* of the TOE ST
  - FCS_RNG.1 (Random number generation): covered by FCS_RNG.1 of the TOE ST
  - FMT_LIM.1/Loader (Limited Capabilities - Loader): no conflicts
  - FMT_LIM.2/Loader (Limited Availability - Loader): no conflicts
  - FIA_API.1 (Authentication Proof of Identity): no conflicts
  - FCS_COP.1/TDES (Cryptographic operation – TDES): no conflicts
  - FCS_CKM.4/TDES (Cryptographic key destruction – TDES): no conflicts
  - FCS_COP.1/AES (Cryptographic operation – AES): no conflicts
  - FCS_CKM.4/AES (Cryptographic key destruction – AES): no conflicts
  - FCS_COP.1/SHA (Cryptographic operation –SHA): covered by FCS_COP.1/SHA of the TOE ST
  - FPT_TST.2 (Subset TOE security testing): covered by FPT_TST.1 of the TOE ST
  - FDP_ACC.1 (Subset access control): covered by FDP_ACC.1/* of the TOE ST
  - FDP_ACF.1 (Security attribute based access control): covered by FDP_ACF.1/* of the TOE ST
  - FMT_MSA.1 (Management of security attributes): used implicitly, no conflicts
  - FMT_MSA.3 (Static attribute initialization): used implicitly, no conflicts
  - FMT_SMF.1 (Specification of Management functions): used implicitly, no conflicts
  - FDP_SDI.1 (Stored data integrity monitoring): no conflicts
  - FCS_COP.1/RSA (Cryptographic Operation – RSA): covered by FCS_COP.1/RSA of the TOE ST
  - FCS_CKM.1/RSA (Cryptographic key management – RSA): covered by FCS_CKM.1/RSA of the TOE ST
  - FCS_COP.1/ECDSA (Cryptographic Operation – ECDSA): covered by FCS_COP.1/EC of the TOE ST
  - FCS_CKM.1/EC (Cryptographic key management – EC): covered by FCS_CKM.1/EC of the TOE ST
  - FCS_COP.1/ECDH (Cryptographic Operation – ECDH): covered by FCS_CKM.1/DH_PACE and FCS_CKM.1/CA of the TOE ST

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

- FCS_COP.1/AES_SCL (Cryptographic operation – AES – SCL): covered by FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC and FCS_COP.1/AES_MAC of the TOE ST
- FCS_CKM.4/AES_SCL (Cryptographic key destruction – AES – SCL): no conflicts
- FCS_COP.1/TDES_SCL (Cryptographic operation – TDES – SCL): no conflicts
- FCS_CKM.4/TDES_SCL (Cryptographic key destruction – TDES – SCL): no conflicts
- FDP_ACF.1/Loader (Security attribute based access control – Loader): no conflicts
- FDP_ACC.1/Loader (Subset access control – Loader): no conflicts

The following table shows the mapping of the security functional requirements of the platform to those of the Composite-ST. Only the SFRs that can be mapped directly are shown.

	FCS_CKM.1/EC	FCS_CKM.1/RSA	FCS_CKM.1/DH_PACE	FCS_CKM.1/CA	FCS_CKM.4	FCS_COP.1/EC	FCS_COP.1/RSA	FCS_COP.1/SHA	FCS_COP.1/PACE_ENC	FCS_COP.1/PACE_MAC	FCS_COP.1/CA_ENC	FCS_COP.1/CA_MAC	FCS_COP.1/AES_MAC	FCS_RNG.1	FDP_ACC.1/*	FDP_ACF.1/*	FPT_EMS.1/*	FPT_FLS.1	FPT_PHP.1	FPT_PHP.3	FPT_TST.1
FRU_FLT.2																		x	x	x	x
FPT_FLS.1																		x	x	x	
FPT_PHP.3																			x	x	
FDP_ITT.1																	x				
FPT_ITT.1																	x				
FDP_IFC.1																	x				
FCS_RNG.1														x							
FCS_COP.1/SHA								x													
FPT_TST.2																					x
FDP_ACC.1															x						
FDP_ACF.1																x					
FCS_COP.1/RSA							x														
FCS_CKM.1/RSA		x																			
FCS_COP.1/ECDSA						x															
FCS_CKM.1/EC	x																				
FCS_COP.1/ECDH			x	x																	
FCS_COP.1/AES_SCL									x	x	x	x	x								

Table 10-5: Mapping of SFRs of the platform to TOE SFRs

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

10.2.2.6 Assurance Requirements

The level of assurance of the

- TOE is EAL4 according to Common Criteria V3.1R5 augmented with ALC_DVS.2 and AVA_VAN.5
- platform is EAL6 according to Common Criteria V3.1R5 augmented with ALC_FLR.1

This shows that the assurance requirements of the platform exceed that of the TOE and thus all assurance requirements of the TOE are met.

10.2.3 Conclusion

Overall there is **no conflict** between **security requirements** of this Composite-ST and the Platform-ST.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

11 References

11.1 General References

[ANSI-X9.62] American National Standard X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), ANSI, 2005-11-16.

[ANSI-X9.63] American National Standard X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, ANSI, 2001-11-20.

[BSI-AIS20-V2] AIS 20 / AIS 31, A proposal for: Functionality classes for random number generators, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.0, 2011-09-18.

[BSI-AIS31-V3] AIS 31, Anwendungshinweise und Interpretationen zum Schema – Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 3, 2013-05-15.

[BSI-AIS36-V4] AIS 36, Anwendungshinweise und Interpretationen zum Schema, AIS36: Kompositionsevaluierung, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 4, 2013-05-15.

[BSI-TR-03110-1-V220] Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.20, 2015-02-26.

[BSI-TR-03110-2-V221] Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2 – Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.21, 2016-12-21.

[BSI-TR-03110-3-V221] Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3 – Common Specifications, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.21, 2016-12-21.

[BSI-TR-03111-V200-ECC] Technical Guideline TR-03111: Elliptic Curve Cryptography, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.00, 2012-06-28.

[BSI-TR-03116-2] TR-03116-2, Technische Richtlinie BSI TR-03116 – Kryptographische Verfahren für Projekte der Bundesregierung - Teil 2: Hoheitliche Dokumente, Bundesamt für Sicherheit in der Informationstechnik (BSI), Stand 2018, 2018-04-23.

[CC-Part1-V3.1] CCMB-2017-04-001, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Common Criteria Maintenance Board, Version 3.1, Revision 5, 2017-04.

[CC-Part2-V3.1] CCMB-2017-04-002, Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Common Criteria Maintenance Board, Version 3.1, Revision 5, 2017-04.

[CC-Part3-V3.1] CCMB-2017-04-003, Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Common Criteria Maintenance Board, Version 3.1, Revision 5, 2017-04.

[CEM-V3.1] CCMB-2017-04-004, Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, September 2012.

[DIR-1999/93/EC] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures. Official Journal of the European Communities, L13:12 – 20, 2000-01-19.

[ICAO-9303-2015] ICAO Doc 9303, Machine Readable Travel Documents – Machine Readable Passports, (this includes the latest supplemental for ICAO Doc 9303 which also should be considered), International Civil Aviation Organization (ICAO), Seventh Edition, 2015.

[ICAO-TR-101] ICAO SAC v1.01, Machine Readable Travel Documents, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, International Civil Aviation Organization (ICAO), Version 1.01, 2010-11-11.

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

[ICAO-TR-110]	ICAO SAC v1.1, Machine Readable Travel Documents, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, International Civil Aviation Organization (ICAO), Version 1.1, 2014-04-15.
[IEEE-1363]	IEEE 1363-2000, IEEE Standard Specifications for Public-Key Cryptography, IEEE Standards Board, 2000-08-29.
[Infineon-Chip-HW-Ref-M7892]	M7892 SOLID FLASH™ Controller for Security Applications, 16-bit Security Controller Family, 90nm Technology, Hardware Reference Manual, Revision 1.7.1, 2015-09-21 and M7892 Errata Sheet, Revision 4.1, 2017-06-21.
[ISO-IEC-11770-3]	ISO/IEC 11770-3:2015, Information technology -- Security techniques – Key management -- Part 3: Mechanisms using asymmetric techniques, ISO/IEC, 2015-08
[ISO-IEC-14443-2018]	ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards – Contactless proximity objects, ISO/IEC, 2018
[ISO-IEC-14888-3]	ISO/IEC 14888_3:2006 – Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, ISO/IEC, 2006-11
[ISO-IEC-7816-part-3]	ISO/IEC 7816-3:2006, Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols, ISO/IEC, 2006-11
[ISO-IEC-7816-part-4]	ISO/IEC 7816-4:2013, Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange, ISO/IEC, 2013-04
[ISO-IEC-9797-1-2011]	ISO/IEC 9797-1:2011, Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher, ISO/IEC, 2011-03
[NIST-FIPS-140-2]	FIPS PUB 140-2, Security Requirements for Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology (NIST), 2001-05-25.
[NIST-FIPS-180-4]	FIPS PUB 180-4, Secure Hash Standard (SHS), Information Technology Laboratory, National Institute of Standards and Technology (NIST), 2012-03-06.
[NIST-FIPS-186-4]	FIPS PUB 186-4, DIGITAL SIGNATURE STANDARD (DSS), Information Technology Laboratory, National Institute of Standards and Technology (NIST), 2013-07.
[NIST-FIPS-197]	FIPS PUB 197, ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology (NIST), 2001-11-26.
[NIST-FIPS-46-3-1999]	FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), U.S. DEPARTMENT OF COMMERCE, National Institute of Standards and Technology (NIST), 1999-10-25.
[NIST-800-38A-2001]	NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, National Institute of Standards and Technology (NIST), 2001 Edition, 2001-12.
[NIST-800-38B-2005]	NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology (NIST), 2005-05.
[NIST-SP800-67]	NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, National Institute of Standards and Technology (NIST), Revision 1, 2012-01.
[NIST-SP800-90A]	NIST Special Publication 800-90A, Recommendation Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology (NIST), Revision 1, 2015-06.
[EU-Reg-910-2014]	eIDAS Regulation (Regulation (EU) No 910/2014), REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Official Journal of the European Communities, L257:73 – 114, 2014-08-28.
[RFC-5639-2010-03]	RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010-03.
[RSA-PKCS1-v2.2]	PKCS #1 v2.2: RSA Cryptography Standard, Version 2.2, 2012-10-27.
[RSA-PKCS-15]	PKCS #15 v1.1: Cryptographic Token Information Syntax Standard, Version 1.1, 2000-06-06.
[RSA-PKCS-3-V1.4]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, 1993-11-01.
[SOG-IS Crypto Catalog-V1.1]	SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms, Version 1.1, 2018-06.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC

11.2 Common Evaluation Evidence

Note: The references in this are common for all evaluated configurations.

[BSI-CC-PP-0056-V2-2012-MA-02]	Assurance Continuity Maintenance Report BSI-CC-PP-0056-V2-2012-MA-02 for Common Criteria Protection Profile / Machine Readable Travel Document with 'ICAO Application', Extended Access Control with PACE (EAC PP), Version 1.3.2, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-12-05.
[BSI-CC-PP-0059-2009-MA-02]	Protection profiles for Secure signature creation device – Part 2: Device with key generation, Information Society Standardization System CEN/ISSS, EN 419211-2:2013, 2013-07-17.
[BSI-CC-PP-0068-V2-2011-MA-01]	Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01, Version 1.0.1, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014-07-22.
[BSI-CC-PP-0071-2012-MA-01]	Protection profiles for Secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, Information Society Standardization System CEN/ISSS, EN 419211-4:2013, 2013-11-27.
[BSI-CC-PP-0072-2012-MA-01]	Protection profiles for Secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, Information Society Standardization System CEN/ISSS, EN 419211-5:2013, 2013-12-04.
[BSI-CC-PP-0084-2014]	Security IC Platform Protection Profile with Augmentation Packages, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.0, 2014-01-13.
[BSI-CC-PP-0086-2015]	Common Criteria Protection Profile / Electronic document implementing Extended Access Control Version 2 defined in BSI TR-03110 [EAC2-PP], Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.01, 2015-05-20.
[BSI-DSZ-CC-0891]	Certification Report, BSI-DSZ-CC-0891-V4-2019 for Infineon Security Controller M7892 Design Steps D11 and G12, with specific IC dedicated firmware and optional software from Infineon Technologies AG, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019-12-19.
[BSI-CC-PP-0035-2007]	Certification Report BSI-CC-PP-0035-2007 for Security IC Platform Protection Profile Version 1.0 from Atmel Secure Products, Infineon Technologies AG, NXP Semiconductors Germany GmbH, Renesas Technology Europe Ltd, STMicroelectronics, Bundesamt für Sicherheit in der Informationstechnik (BSI), V1.0, 2007-06-15.
[Infineon-ST-M7892-D11-G12]	Security Target Lite, M7892 Design Steps D11 and G12, Common Criteria EAL6 augmented / EAL6+, Version 1.2, 2017-11-21.
[Atos-V54DI-QES-LC-Support]	Life Cycle Support 'CardOS DI V5.4 QES Version 1.0', Atos Information Technology GmbH
[Atos-V54DI-QES-Adm-Guid]	Administrator Guidance 'CardOS DI V5.4 QES Version 1.0', Atos Information Technology GmbH
[Atos-V54DI-QES-User-Guid]	User Guidance 'CardOS DI V5.4 QES Version 1.0', Atos Information Technology GmbH
[Atos-V54DI-QES-AQES]	Application QES 'CardOS DI V5.4 QES Version 1.0', Atos Information Technology GmbH
[Atos-V54-CardOS-Users-Manual]	CardOS V5.4 User's Manual, Atos Information Technology GmbH
[Atos-V54DI-CardOS-PR-Notes]	CardOS DI V5.4 Package & Release Notes, Atos Information Technology GmbH

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

Appendix A: Overview Cryptographic Algorithms

This TOE is a composite product and uses for cryptographic mechanism listed only mechanism provided by the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12) except for SHA-224 and SHA-384, see note 6 below. The "Standard of Implementation" is a citation of the ST of the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12) only, cf. [Infineon-ST-M7892-D11-G12].

The following cryptographic algorithms are used by the TOE to enforce its security policy:

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in bits	Standard of Application	Comments ST Reference
1	Authenticity	RSA-signature generation (RSA PKCS1_v1_5, RSA PSS), using SHA-224, SHA-256, SHA-384 or SHA-512	[RSA-PKCS1-v2.2], [NIST-FIPS-186-4]	2048, 3072	[SOG-IS Crypto Catalog-V1.1]	Digital signature creation FCS_COP.1/RSA (see note 2)
2		ECDSA-signature generation, using SHA-256, SHA-384 or SHA-512 (depending on curve)	[BSI-TR-03111-V200-ECC], [NIST-FIPS-186-4], [RFC-5639-2010-03]	Key sizes corresponding to the used elliptic curves: NIST P-256, NIST P-384, NIST P-521 BP P256r1, BP P384r1, BP P512r1	[SOG-IS Crypto Catalog-V1.1]	Digital signature creation FCS_COP.1/EC (see note 2)
3	Authentication	PACEv2 (Generic Mapping), Password Authenticated Connection Establishment	[BSI-TR-03110-1-V220] (PACE v2)	128 (nonce) $\log_2(10^n\text{-}1)$ (n = length of PIN_CH, PUK_CH, PIN.T, CAN, PIN_ADMIN), see note 7	[ICAO-TR-110], [BSI-TR-03110-1-V220]	FCS_CKM.1/DH_PACE, FCS_CKM.1/DH_PACE (see note 3)
4		Symmetric Authentication, AES in CMAC mode	[NIST-FIPS-197] (AES), [ISO-IEC-9797-1-2011] algorithm 5 and padding method 4 (CMAC)	128, 192, 256	[ICAO-TR-110], [BSI-TR-03110-1-V220]	FCS_COP.1/AES_MAC (see note 4)
5		Implicit authentication during SM, AES in CBC mode	[NIST-FIPS-197] (AES), [NIST-800-38A-2001] section 6.2 (CBC)	192, 256	[ICAO-TR-110], [BSI-TR-03110-1-V220]	FCS_COP.1/PACE_ENC session key after PACE secure messaging (see note 4)
6	Key Generation	EC signature key pair generation	ECDSA Key Generation appendix A4.3 in [ANSI-X9.62], section 6.4.2 in [ISO-IEC-14888-3] and appendix A.16.9 in [IEEE-1363]	Key sizes corresponding to the used elliptic curves: NIST P-256, NIST P-384, NIST P-521 BP P256r1, BP P384r1, BP P512r1	[SOG-IS Crypto Catalog-V1.1]	FCS_CKM.1/EC (see note 3)
7		RSA signature key pair generation	Proprietary. Generated keys meet [RSA-PKCS1-v2.2], sections 3.1 and 3.2 and [IEEE-1363], section 8.1.3.1	2048, 3072	[SOG-IS Crypto Catalog-V1.1]	FCS_CKM.1/RSA (see note 3)
8	Key agreement	PACE ECDH Key Agreement	[NIST-FIPS-186-4], [ANSI-X9.63]	Key sizes corresponding to the used elliptic curves: NIST P-256, NIST P-384, NIST P-521	[ICAO-TR-110], [BSI-TR-03110-1-V220]	FCS_CKM.1/DH_PACE (see note 3)

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in bits	Standard of Application	Comments ST Reference
				BP P256r1, BP P384r1, BP P512r1		
9		PACE Key derivation using SHA-256	[ICAO-TR-110], [ANSI-X9.63]	192 (AES), 256 (AES)	[ICAO-TR-110], [BSI-TR-03110-1-V220]	FCS_CKM.1/DH_PACE (see note 3)
10		Chip Authentication Key Agreement	[NIST-FIPS-186-4], [ANSI-X9.63]	Key sizes corresponding to the used elliptic curves: NIST P-256, NIST P-384, NIST P-521 BP P256r1, BP P384r1, BP P512r1	[ICAO-TR-110], [BSI-TR-03110-1-V220]	FCS_CKM.1/CA (see note 3)
11		Chip Authentication Key derivation using SHA-256	[ICAO-TR-110], [ANSI-X9.63]	192 (AES), 256 (AES)	[ICAO-TR-110], [BSI-TR-03111-V200-ECC]	FCS_CKM.1/CA (see note 3)
12	Confidentiality	Secure Messaging, AES in CBC mode	[NIST-FIPS-197] (AES), [NIST-800-38A-2001] section 6.2 (CBC)	192, 256	[ICAO-TR-110], [BSI-TR-03110-1-V220]	FCS_COP.1/PACE_ENC, FCS_COP.1/CA_ENC (see note 4)
13	Integrity	Secure Messaging, AES in CMAC mode	[NIST-FIPS-197] (AES), [ISO-IEC-9797-1-2011] algorithm 5 and padding method 4 (CMAC)	192, 256	[ICAO-TR-110], [BSI-TR-03110-1-V220]	FCS_COP.1/PACE_MAC, FCS_COP.1/CA_MAC (see note 4)
14	Trusted Channel	Secure Messaging in ENC MAC mode established during PACE	[BSI-TR-03110-1-V220]	see No. 9 - 12	[ICAO-TR-110], [BSI-TR-03110-1-V220]	FTP_ITC.1/SCD FTP_ITC.1/VAD FTP_ITC.1/DTBS
15	Cryptographic primitive	DRG.4 random number generator	[BSI-AIS20-V2], [NIST-FIPS-197] (AES), random source of class PTG.2 according to [BSI-AIS31-V3]	-	[BSI-TR-03116-2],	FCS_RNG.1 for PACE additionally processed according to [BSI-TR-03116-2] section 1.3.3.1 (see note 5)
16		SHA-224, SHA-256, SHA-384, SHA-512	[NIST-FIPS-180-4]	-	[BSI-TR-03110-1-V220]	Signature verification, signature generation, key derivation (see note 6)

Notes:

1. This TOE uses the Infineon libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010 of the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12). For the standard of implementation of "digital signature verification" using RSA or EC see [Infineon-ST-M7892-D11-G12]
2. This TOE uses the Infineon libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010 of the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12). For the standard of implementation of "digital signature generation" using RSA or EC see [Infineon-ST-M7892-D11-G12].
3. This TOE uses the Infineon libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010 of the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12). For the "cryptographic key generation algorithm" for RSA, EC and ECDH see [Infineon-ST-M7892-D11-G12]
4. This TOE uses the Infineon libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010 of the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12). For the standard of implementation of "Advanced Encryption Standard (AES)" see [Infineon-ST-M7892-D11-G12]
5. This TOE uses the random numbers generation provided by the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12) as random source for the hybrid deterministic random number generator. For the standard

Copyright © Atos Information Technology GmbH 2020. All rights reserved.

of implementation of "random numbers generation Class DRG.4 according to [BSI-AIS20-V2]" see [Infineon-ST-M7892-D11-G12]

6. This TOE uses the Infineon libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010 of the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12). For the standard of implementation of hash algorithms SHA-{256, 512} see [Infineon-ST-M7892-D11-G12].
   The hash algorithm SHA-224 is provided by CardOS DI V5.4 using a SHA-256 value according to [NIST-FIPS-180-4] section 6.3.
   A SHA-384 value is computed by CardOS DI V5.4 from a SHA-512 value according to [NIST-FIPS-180-4] chapter 6.5.
7. Formula holds for the assumption, that only digits are used.
8. This TOE uses the Infineon libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010 of the underlying chip SLE78CLFX*P* (M7892 Design Steps D11 and G12). For computing the shared secret the modular exponentiation function (cryptorsasignexp) of the RSA crypto library is used. Function "cryptorsasignexp" of RSA crypto library is used also for signing.

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

According to [ICAO-9303-2015], [ICAO-TR-110], [BSI-TR-03110-1-V220], and [BSI-TR-03110-3-V221] the algorithms are suitable for authenticity, authentication, key agreement, confidentiality and integrity. An explicit validity period is not given.

However according to [SOG-IS Crypto Catalog-V1.1] for RSA signature generation the acceptability deadline for the legacy use of modulus of size above 1900 bits, but less than 3000 bits, is set to (31 december) 2024. For other algorithms the default acceptability deadline for legacy mechanisms is set to (31 december) 2022.

Copyright © Atos Information Technology GmbH 2020. All rights reserved. PUBLIC