Certificate Policy / Certification Practice Statement (CP/CPS)

for the Issuance of Certificate of the Classes

„Diamant“ (qualified) and „Saphir“ (advanced)

Version: 3.5

Date: December 22nd, 2021

Swisscom IT Services Finance S.E. ("Swisscom ITSF")
Mariahilfer Strasse 123/3
A-1060 Wien

Document history

Version	Date	Changed by	Comments/nature of the change
3.0	05.04.2017	Kerstin Wagner, H-P Waldegger, Stéphane Vaucher	Creation of a CP/CPS according to eIDAS-VO and the new ETSI-Standards (German Version).
3.0	24.05.2017	Governance Board	Approval of the German version
3.0	15.06.2017	Kerstin Wagner, H-P Waldegger	Compilation of the English version
3.1	19.04.2018	Kerstin Wagner, H-P Waldegger	Updating of the CRL and OSCP update intervals; updating of the PKI hierarchy; specification of the approved documents and procedures for issuing qualified certificates; description of communication in the event of changes.
3.1	15.06.2018	Governance Board	Approval
3.2	16.10.2018	H-P Waldegger	Various clarifications after audit and update CA 4
3.2	19.11.2018	Governance Board	Approval
3.3		Kerstin Wagner H-P Waldegger	Additions to the root CA 4 hierarchy, extension to additional means of authentication and obligation of the registries to submit an implementation concept.
3.3	22.01.2020	QTSP Board	Approval
3.4	15.06.2020	H-P Waldegger	Limitation of liability chap. 9.7.1 supplemented
3.4	18.01.2021	QTSP Board	Approval
3.4	15.03.2021	Ingolf Rauh	Translation into English
3.5	03.06.2021	Kerstin Wagner	Correction of the OID of Root CA 2; Backup locations adjusted, new CA hierarchy, Updating CRL and OCSP service, updating and supplementing regulations.
3.5	22.12.2021	QTSP Board	Approval

Referenced Documents

[eIDAS-VO]	Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[SVG]	Austrian Federal Law on electronic signatures and trust services for electronic transactions (Signature- and Trust Services Law)
[SVV]	Austrian Ordinance on electronic signatures and trust services for electronic transactions (Signature- and Trust Services Ordinance)
[RFC 3647]	IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework"
[RFC 5280]	IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
[RFC 6960]	IETF RFC 6960: "Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol – OCSP"
[CEN EN 419 241-1]	Trustworthy Systems supporting Server Signing; Part 1: General Security Requirements
[ETSI TS 119 312]	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[ETSI EN 319 401]	General Policy Requirements for Trust Service Providers
[ETSI EN 319 411-1]	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI EN 319 411-2]	Policy and security requirements for TSPs; Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETSI EN 319 421]	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[ETSI EN 319 412-1-5]	Certificate Profiles
[Addendum EU]	Addendum to the CP/CPS: Profiles of Certificates, Revocation Lists (CRL) und Online Status queries (EU)
[Security Concept]	Security Concept SDCS
[Role Concept]	Role Concept SDCS

swisscom

Table of Contents

1 Introduction

This document (hereinafter referred as "CP/CPS") sets out the Certificate Policy (CP) and the Certification Practice Statement (CPS) of Swisscom IT Services Finance S.E. for issuing certificates complying with the EU Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [eIDAS-VO], the Austrian Federal Law on electronic signatures and trust services for electronic transactions [SVG] and the related ordinance on electronic signatures and trust services for electronic transactions [SVV].

Swisscom IT Services Finance S.E. (hereinafter referred to as "Swisscom ITSF") operates as a qualified trust service provider a trust service issuing advanced and qualified certificates for use for advanced and qualified electronic signatures and advanced and qualified electronic seals as well the issuing of qualified time-stamps.

The present CP/CPS refers to different certificate classes, "Diamant" for qualified certificates and "Saphir" for advanced certificates, and also to two different CA generations. The second-generation CAs under the root CA 2 have reached the end of their lifecycle, while the CAs under the root CA 4 with current algorithms and key lengths can withstand the requirements of the next few years.

If not otherwise indicated all specifications in this document apply to both certificate classes.

1.1 Overview

The structure of this CPS is based on the guidelines set out in [RFC 3647].

This CP / CPS complies with the following standards of the European Institute for Telecommunications Standards for qualified trust service providers:

- ETSI EN 319 411-1 (2018-04): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements; [ETSI EN 319 411-1]
- ETSI EN 319 411-2 (2018-04): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates; [ETSI EN 319 411-2]
- ETSI EN 319 421 (2016-03): Policy and Security Requirements for Trust Service Providers issuing Time-Stamps; [ETSI EN 319 421]

This English translation of the CPS has been prepared to facilitate international cooperation with other trust service providers; however, the most recent German version always takes precedence.

1.2 Document Identification

Title:	Swisscom Digital Certificate Services - Certificate Policy / Certification Practice Statement for the Certificate Classes „Diamant“ (qualified) and „Saphir“ (advanced)	
Version:	3.5	
Object Identifier:	2.16.756.1.83.2.1	Root CA of generation 2
	2.16.756.1.83.30.4.0	Root CA of generation 4
	2.16.756.1.83.100.4.1	Diamant EU CA of generations 4 and 4.1
	2.16.756.1.83.100.4.2	Saphir EU CA of generations 4 and 4.1

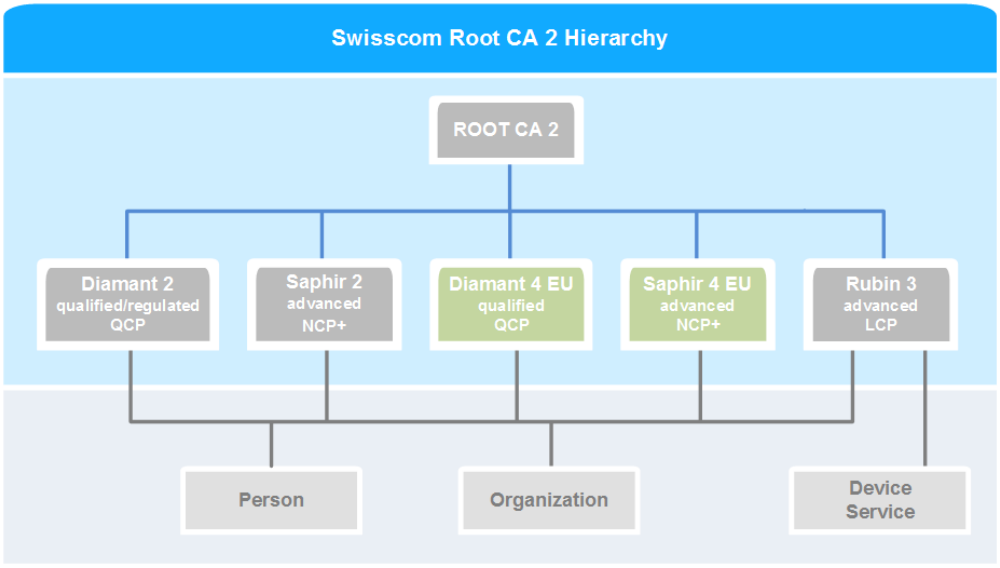
If certificates contain additional digits in the OID, this refers to the version number of this document that is valid for the certificate.

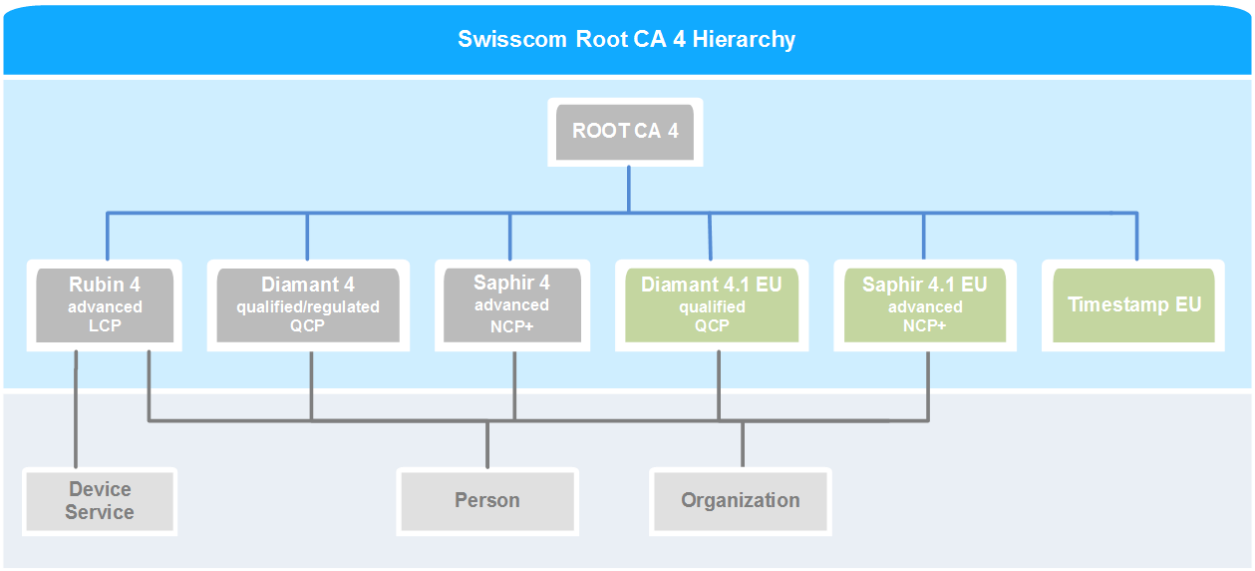
The OID of Swisscom Digital Certificate Services is based on the RDN assigned by the Swiss Federal Office of Communications (OFCOM).

1.3 Participants of the PKI

1.3.1 Certificate Authorities (CA)

The Public Key Infrastructure (PKI) of Swisscom ITSF is structured hierarchically:





Responsible for the CAs shown here in green and marked with the addition "EU" is Swisscom ITSF with its registered office in Vienna. These CAs comply with European and Austrian legislation. The CAs shown in grey fulfil the very similar requirements from Swiss legislation and are the subject of a separate certificate policy.

The PKI presented here is operated exclusively by Swisscom (Switzerland) Ltd. All systems are located in Switzerland.

Root-CA

The Swisscom Root-CA is not connected to any network and is only started when required. The Root-CA only issues certificates for subordinate Certificate Authorities (CA) of Swisscom ITSF.

The following CAs of Swisscom ITSF are operated below the root CA:

Diamant EU CA (qualified)

Issuing certificates of the class "Diamant" for natural and legal persons. Meets the requirements of qualified certificates for electronic signatures for natural persons as set out in art. 3 para 15 [eIDAS-VO] and for electronic seals for legal persons as set out in art. 3 para 30 [eIDAS-VO] and uses a secure cryptographic device (QSCD).

Saphir EU CA (advanced – NCP+)

Issuing certificates of the class "Saphir" for natural and legal persons. Meets the requirements of certificates for advanced electronic signatures for natural persons as set out in art. 3 para 11 [eIDAS-VO] and for electronic seals for legal persons as set out in art. 3 para 26 [eIDAS-VO] and uses a secure cryptographic device (SCD).

Time-Stamping-Service CA (qualified)

For creating and signing the certificates of the time-stamping units (TSU). Meets the requirements of qualified time-stamps as set out in art. 3 para 34 [eIDAS-VO].

1.3.2 Registration Authorities (RA)

The registration authorities identify and authenticate applicants, record and verify the applications for various certification services, archive the application documentation (verified documents, power of attorney, etc.) and forward the data to the certification authority. Swisscom ITSF may delegate the task of registration to third parties (hereinafter "RA Partner"). RA partners are obliged by contract to comply in particular with the processes for the registration, issuing of certificates, revocation and archiving defined in this document. For each RA partner, an implementation concept describes the procedures used in their context to comply with these obligations.

1.3.3 Subscribers

Subscribers are natural or legal persons who can be clearly identified by the name defined in the certificate. The subscriber is the person or organization who owns the private key of the certificate and who is the subject of an electronic signature or electronic seal based on this certificate.

Swisscom ITSF may issue certificates for itself and act as subscriber. The same requirements apply to Swisscom ITSF as for all other subscribers.

1.3.4 Relying Parties

Relying parties are natural or legal persons (such as legal entities and authorities) that use the certificates of this PKI (e.g. verification of the validity of a signature) and have access to the certification services of Swisscom ITSF.

1.3.5 Other participants

Other participants can be natural persons or organizations (such as legal entities and authorities), who are involved in the certification or registration process as service providers.

1.4 Certificate Usage

1.4.1 Permitted Certificate Usage

The certificates shall only be used for the applications which are in accordance with the usage specified in the certificate (keyUsage).[1]

The advanced certificates "Saphir" issued under this CP / CPS can be used to create advanced electronic signatures or advanced electronic seals.

The qualified certificates "Diamant" issued under this CP / CPS can be used to create qualified electronic signatures or qualified electronic seals

The keys of the root CA are used exclusively for signing CA certificates and revocation lists.

The private keys of issuing CAs are used to sign the associated end user certificates and OCSP signer certificates.

1.4.2 Prohibited Certificate Usage

Types of use that do not correspond to the use specified in the certificate (keyUsage) are not permitted. Swisscom ITSF shall not be liable for damages resulting from the use of the services beyond these restrictions.

The use of the certificates for the creation of qualified electronic signatures for certificate applications according to eIDAS Regulation Art 24 (1) c is prohibited.

1.5 Policy administration

Publisher of this document:

Swisscom IT Services Finance S.E.
Swisscom Trust Services
Mariahilfer Strasse 123/3
A-1060 Wien

Changes to this CP / CPS are approved by the QTSP Board of Swisscom Digital Certificate Services and notified to the supervisory body.

1.6 Definitions and Acronyms

Term	Explanation
Certificate Authority (CA), Issuing CA	Issuing CAs are used to provide certificates to users, computers, and other services.
Certificate Policy (CP)	A set of rules which require the applicability of a certificate for a particular group of persons and / or a class of specific applications with joint security requirements.
Certificate Revocation List (CRL)	List signed by the CA containing the serial numbers of all certificates which have been declared invalid before the expiry of their validity.
Certificate Status Management	Service of the TSP, by means of which the users of a certificate can check whether it has been declared invalid.

[1] The highlighted frames are subsequently used to assign rules for a specific certificate class - orange for "Diamant" and blue for "Saphir".

Term	Explanation
Certification Practice Statement (CPS)	Statement on the rules and practices effectively applied by the TSP to issue certificates. The CPS defines the devices, the policy and the procedures used by the TSP in accordance with its chosen certificate policy.
Conformity assessment body	A body accredited by the supervisory body of an EU Member State that verifies and certifies the conformity of qualified trust service providers and the qualified trust services they provide.
Digital certificate	Electronic certificate that associates a signature verification key with the name of a person, an organisation or a device.
Electronic or digital signature	Technical procedure for verifying the authenticity of a document, an electronic message or the identity of the sender. The electronic signature and the handwritten signature are considered to be partially equivalent in the case of the use of digital certificates as defined in art. 4 [SVG].
Electronic signature or seal creation device	Software / firmware or hardware configured to implement the signature key used by the subscriber to create an electronic signature or seal, e.g. a SmartCard or a HSM.
Hash	The hash function is a cryptographic checksum for a text to ensure its integrity. The method is used to reduce the computational effort when encrypting data using the public key method. A hash function generates a fixed-length checksum (hash value) which is applied to the message having a variable length. Thus the integrity of a message can be identified with no doubt.
HSM (High Security Module)	Device for the efficient and secure execution of cryptographic operations or applications. HSM offer extensive functions for secure management of the device and the key material. HSMs are certified according to security standards, such as FIPS 140-2 or Common Criteria (CC).
Issuing of certificates	Service of the TSP; issuing of a digital certificate based on the name of the applicant of a certificate and of his / her attributes, which are verified during the registration.
Key pair, key material	Signature key and associated signature verification key, which are mathematically linked by an asymmetric signature algorithm.
„On Demand“ issuing and use of key material	„On Demand“ issuing and use of key material (private and public keys as well as certificates), that are used for electronic signature. The key pairs are created and used in a secure environment (QSCD) and deleted immediately after the signature they have been created for.
QTSP	Qualified Trust Service Provider
Qualified certificate	Digital certificate, that meets the requirements set out in appendix I [eIDAS-VO].
Qualified electronic seal	The "Qualified Electronic Seals" is an advanced electronic seal that is created by a qualified electronic seal creation device, and which is based on a qualified certificate for electronic seals (Art. 3 para 27 [eIDAS-VO])
Qualified electronic signature	The "Qualified Electronic Signature" is 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 (Art. 3 para 12 [eIDAS-VO])
Qualified electronic signature or seal creation device	Signature or seal creation device, that meets the requirements set out in appendix II [eIDAS-VO].
RDN names, Relative Distinguished Name	Names of the directory entries whose unambiguousness refers to a particular entry and which are components of a directory name (distinguished name).
Registration	Service of the registration authority, which is to verify the identity and, if necessary, the attributes of each applicant of a certificate before his / her certificate is generated or the activation data (or password) is assigned to activate the use of the signature key.
Relying Party	Person or process which, when using this certificate, relies on the verified electronic signatures or seals.

Term	Explanation
Revocation of a certificate	Service of the TSP, which withdraws the validity of a certificate before its expiry.
Security Policy (SP)	A set of rules and guidelines drawn up on the basis of a risk analysis to reduce the likelihood of possible incidents (preventive measures) and to address the impact of such incidents (corrective measures) in order to identify and protect the resources valuable for the trust service provider. With the security strategy and policy, the overall security level to be achieved for an information system and especially for each component of the security architecture can be clearly defined.
Signature key (private key)	Unique data, such as codes or private cryptographic keys, used by the subscriber for creating an electronic signature or seal.
Signature verification key (public key)	Data such as codes or public cryptographic keys used for verifying an electronic signature or seal.
Subscriber	Natural and legal person who is the owner of the signature key assigned to the signature verification key listed in the certificate.
Supervisory body	Each Member State of the EU shall appoint a supervisory body which performs the supervisory tasks in the designating Member State, e.g. the accreditation of conformity assessment bodies (certification body) and supervise the qualified trust service providers established in its territory. In Austria, the Telecom Control Committee is the supervisory body for trusted service providers.
Time-stamp object receiver (relying party)	Recipient of a time stamp object that trusts this time stamp object
Time-stamp object, Time-stamp token	Data object that links the representation of a fact to a particular point in time and thus provides the proof that the fact existed before the time.
Time-stamp service user (subscriber)	Natural person who stamps his own or data of a legal person or organization through a time stamp service.
Time-stamping	Service of the TSP, which provides an attestation bearing the date, time and a qualified signature, according to which certain digital data have existed at a given time.
Time-stamping Authority (TSA)	Instance that creates timestamp objects.
Time-stamping Policy (TP)	Specification of general processes used by the time-stamping service during the creation of signed timestamps.
Time-stamping unit	IT infrastructure, which is used to create time stamp objects. On this infrastructure, there is only one private key for issuing time stamp objects.
Trust Center	Specially protected room where the TSP infrastructure is operated
Trust Service Provider (TSP)	An organization that issues digital certificates and / or provides other signature and certification services.
TSA Practice Statement (TPS)	Information on the rules and guidelines, which are effectively implemented by the TSP for the issuance of time stamp objects. The TPS defines the equipment, methods, and procedures applied by the Time-stamp service provider to issue and manage timestamp objects according to [eIDAS-VO] and Swiss signature law.
UTC, coordinated Universal Time	Universal time scale based on seconds. UTC is defined in the ITU-R recommendation TF.460-

1.7 Abbreviations

AIS	All-in Signing Service
BCP	Business Continuity Plan
CA	Certification Authority
CSIRT	Computer Security Incident Response Team
CN	Common Name, part of the DN
CP	Certificate Policy,
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name as per RFC 3739
EAL	Level of trustworthiness (Evaluation Assurance Level) according to Common Criteria
EAL4+	Requirements according to test level EAL 4, extended by the insurance element AVA_VAN.5 (Advanced methodical vulnerability analysis).
eIDAS-VO	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 1999/93/EG
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
ISO	Information Security Officer
LDAP	Lightweight Directory Access Protocol
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol, service for online validation of certificates
OID	Object Identifier
PDS	PKI Disclosure Statement
PED	PIN Entry Device
PIN	Personal Identification Number
QCP-l-qscd	Policy for EU qualified certificates issued to legal persons, where the private key and the related certificate reside on a QSCD
QCP-n-qscd	Policy for EU qualified certificates issued to natural persons, where the private key and the related certificate reside on a QSCD
RA	Registration Authority,
Re-key	renewing a certificate using a new key pair
QSCD	Qualified electronic Signature/Seal Creation Device, as set out in ISO/IEC 15408
QTSP	Qualified Trust Service Provider
SSL	Secure Socket Layer
SVG	Austrian Federal Law on electronic signatures and trust services for electronic transactions (Signature- and Trust Services Law)
SVV	Austrian Ordinance on electronic signatures and trust services for electronic transactions (Signature- and Trust Services Ordinance)
TLS	Transport Layer Security
TSA	Time-stamping Authority
TSP	Trust Service Provider
TSU	Time-stamping unit

2 Publications and Repository Responsibility

2.1 Repository Service

Swisscom ITSF provides its Root and CA certificates, blocking lists (CRL) of the Root CAs, CP / CPS documents and terms of use on the web.

The repository of the Swisscom Trust Services is located at:

https://trustservices.swisscom.com/en/repository

The online services for querying the information listed in chapter 2.2 are available 24x7 with an availability of 99.9%.

2.2 Publication of Information

The following information is published on Swisscom's website:

- CP/CPS documents
- Terms and Conditions of Use
- Certificates of the Root-and Issuing CAs as well as TSS CA and TSUs
- Certificate revocation lists of the Root CAs
- Revocation information in case of a compromise of the root CA

Adaptations in these documents are communicated according to the specifications in chapter 9.8.4.

Other certificates (especially end user certificates) are not published publicly.

2.3 Frequency of Publication

Newly issued certificates, CRLs, guidelines and any other applicable information is promptly made available. The following publication frequencies apply:

- Certificate revocation lists (CRL) of the Root CAs: as required, but at least once a year
- CP / CPS documents: following amendments resp. after approval of the document
- Other information: as required

2.4 Access Controls on Repositories

The information in chapters 2.1 and 2.2 is publicly available.

3 Identification and Authentication

3.1 Naming

The identity of the certificate holder is described in the certificate by a unique name (Distinguished Name, DN) according to the standard series X.500. A DN consists of several mandatory and optional name elements.

Selectable name elements must not be abusive nor insinuating and should not infringe third party rights (in particular, naming rights) or other legal norms. The registration office is not obliged to check the DN for conformity with third party rights, the certificate holder alone is responsible for such verifications. If Swisscom ITSF or the registration authority is informed of an infringement of such rights, Swisscom ITSF may declare the certificate invalid.

3.1.1 Name Components Required for Natural Persons

The DN of natural persons must consist of country, common name and either first / last name or pseudonym and can be extended with optional elements according to section 3.1.3.

Element	X.520 attribute	Content	Description
Country	countryName (C)	Two-digit ISO 3166 country code	Country in which the subscriber is domiciled, or the presented identity document of the subscriber has been issued or in which the subscriber has a financial relationship (e.g. bank account).
Common name	commonName (CN)	Informal name of the subscriber for general presentation.	A representation of the name, as the subscriber or the TSP considers it appropriate and comprehensible for user- or system-friendly presentation.
Identity *either first and last name*	givenName	Formal first name(s) of the subscriber	Exact reproduction of the contents of the corresponding field from the presented identity document.
	surName	Formal last name of the subscriber	Exact copy of the content of the corresponding field from the presented identity document.
or	pseudonym	Abstract string / alias	Any string that uniquely identifies the certificate holder in the context of the PKI. The identity of the holder does not need to be recognizable without additional information from the certificate.
Uniqueness	serialNumber	Abstract string, which ensures the uniqueness of the DN	Character string according to one of the following definitions: • Serial number assigned by Swisscom • Serial number assigned by a Registration Authority with a specific prefix managed by Swisscom • Character string according ETSI EN 319412-2 of "Natural person semantics identifier" If a pseudonym is used, which ensures the unambiguity, the serialNumber can be omitted.

3.1.2 Name Components Required for Legal Persons

The DN of a legal person must consist of country, common name, company (names) according to the entry in the commercial register and an identifier derived from the company tax identification number (UID) and can be extended with optional elements according to section 3.1.3.

Element	X.520 attribute	Content	Description
Country	countryName (C)	Two-digit ISO 3166 country code	Country in which the subscriber is domiciled, or the presented identity document of the subscriber has been issued or in which the subscriber has a financial relationship (e.g. bank account).
Common name	commonName (CN)	Informal name of the subscriber for general presentation	A representation of the name, as the subscriber or the TSP considers it appropriate and comprehensible for user- or system-friendly presentation.

Element	X.520 attribute	Content	Description
Identity	organization Name (O)	Formal company (name of the businessperson under which he operates his business) of the subscriber	Exact copy of the content of the corresponding field from the presented identity document.
Uniqueness	organization Identifier	String derived from the official register number of the organization	Character string according **ETSI EN 319412-3** of "Legal person semantics identifier"

3.1.3 Optional Name Components

X.520 attribute	Content	Description
organization Name (O)	Identifying organization	In the case of natural persons, an organization description can be added which ensures the uniqueness of the name. Further interpretations of the relationship of the certificate holder to the organization are not permissible.
organizational Unit (OU)	Part within the organization.	If an organization (O =) is specified, one or more organizational units can be defined by the designated organization. The role and ratio of the certificate holder to the organizational units is not defined.
stateOr ProvinceName (ST)	Province / State	Geographical sub-area of the country (C =) where the subscriber has his / her (residential) seat or the presented identification document of the subscriber has been issued.
localityName (L)	Town	The town where the subscriber is domiciled, or the presented identity document of the subscriber has been issued.
emailAddress	An e-mail-address of the subscriber	The e-mail address given by the subscriber and administered by the subscriber at the time of the identification.

3.1.4 Test-Certificates

Certificates for test purposes are permitted in exceptional cases if their exhibition is necessary for the preparation or the examination of the regular productive use. The number of test certificates is to be kept low. The test certificates must contain the expression "TEST" in the common name (CN) as well as in any organization description.

Pseudonyms are not allowed for test certificates.

3.2 Initial Identity Validation

3.2.1 Identification for Applications by Natural Persons

For the identity validation of the applicant for advanced certificates, the following procedural steps shall be performed:

- For the identity validation, the applicant must provide either an official photo identification or another equivalent proof of identity. Accepted as equivalent, among others, are
  a. "Gelbe Identifikation" of the Swiss Post;
  b. POSTIDENT-proof of the Deutsche Post;
  c. Confirmation of the identity of an account-based payment service provider subject to the Payment Services Directive 2 (2015/2366) of the European Parliament;
  d. The indication of a mobile telephone connection to be used in relation with the certification services, subject to the following conditions:

- The applicant shall provide proof that he is the holder of the connection or otherwise has access to the connection (in the case of a connection contract with a different name, such as a business telephone);
- It is a connection of a telecommunication service provider, which is subject to the Swiss Telecommunications Law;

e. Application forms electronically signed by an accredited trust service provider.

- The registration authority reviews the documents submitted and validates their compliance with the information contained in the application.
- The registration authority performs the identity check based on the proof of identity provided. The expiration date of the submitted documents, name, first name and all attributes to be entered in the certificate are checked.
- The registration authority assigns or checks the existence and correctness of the applicant's authentication means and registers it as a legitimate authentication means for later adjustments of the user data and as a method for the release of remote signatures of Swisscom ITSF. The authentication means shall be approved by Swisscom and shall comply with Sole Control Assurance Level 1 as described in [CEN EN 419 241-1].
- The applicant confirms his acknowledgement of the procedure described above and the acceptance of the Swisscom ITSF Terms and Conditions of Use for the relevant Certificate Class.

For applications for qualified certificates, the following additional requirements apply:

1. The applicant must be present in person or another procedure which is certified by the Austrian supervisory body in accordance with Article 24 para. 1 [eIDAS-VO] must be used.
2. the registration and use of the authentication means must be carried out using a procedure that complies with level 2 (Sole Control Assurance Level 2) described in [CEN EN 419 241-1] according to a recognized assessment body. The procedure may only be used in combination with Swisscom ITSF remote signatures after presentation of such a certificate.

The certificate application, proof of identity and consent to the Terms and Conditions of Use are archived according to the information in section 5.5.2.

If the application comprises the inclusion of an organization name (O =) in the DN, the following additional checks are conducted:

1. Confirmation of the consent of the organization to use the desired name elements in the certificate;
2. Proof of company or name rights of the organization to the requested organization name.

If the applicant already has a valid certificate, the application for further certificates of the same quality can also be made by sending an electronically signed application form. The prerequisite for this type of application is that no more than five years have elapsed since the initial application of the valid certificate, and the identity document (official photo identification) presented during identification was still valid.

Applications for personal certificates may only be made for oneself (no representation).

3.2.2 Identification for Applications by Legal Persons

The following procedural steps are applicable for the validation of applications by legal persons for advanced certificates:

1. The representative of the applicant must be a natural person (also several natural persons can jointly exercise the representation, in particular in regard to collective signing):
    a. In the case of a personal appearance, the identity of the representatives is determined as set out in section 3.2.1 in accordance with the requirements of the requested certificate class.
    b. If the application is electronically signed by the representatives, it is ensured that the certificate class used corresponds at least to the requested certificate class.
2. The representative of the applicant shall submit:
    a. An extract from the company register or an actual extract from the register of the registration agency that registers the organization for the country in question
    b. If he is not registered in the commercial register as a sole authorized signatory: a power of attorney to issue a certificate application, supplied by the managing body of the applicant (for example, the board of directors or the management), or persons registered as authorized signatory in the company register.
3. The registration authority reviews the submitted documents and validates their compliance with the information contained in the application (in particular the extract from the company register, authority).
4. The registration authority verifies the presence and compliance with the technical minimum requirements of the SSL client certificate provided by the applicant as a legitimate authentication means as a method for the approval of remote signatures of the Swisscom ITSF.
5. The applicants confirm their acknowledgement of the -described procedure above and the acceptance of the Swisscom ITSF Terms and Conditions of Use for the relevant Certificate Class

For applications for qualified certificates, the following additional requirements apply:

1. The representative of the applicant must be present in person or a procedure has to be used which has been approved in Austria in accordance with Article 24 para. 1 [eIDAS-VO].
2. The registration and use of the authentication means must be carried out using a procedure described by the applicant, which is approved by Swisscom and corresponds to level 2 (Sole Control Assurance Level 2) described in [CEN EN 419 241-1].

The certificate application, proof of identity and consent to the Terms and Conditions of Use are archived according to the information in section 5.5.2.

3.2.3 Non-verified Information

All information that is included in the certificate is checked. No other information is checked beyond that.

3.2.4 Method for proving Possession of Private Key

The private keys are generated within a secure cryptographic device (HSM) on the protected infrastructure of Swisscom. Certificates created in this way do not require a procedure for proving possession of the private key.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

If all the documents submitted for the identification are still available and no attributes which have not yet been checked are to be included in the new certificate, no additional measures are necessary for the identification of the applicant of a re-key request. The prerequisite for this type of application is that the registration authority has validated the applicants' identity as described in chapter 3.2 within the last five years.

Applications for personal certificates may only be made for oneself (no representation).

For all other cases, proceed as for a new application (chapter 3.2).

3.3.2 Identification and Authentication for Re-Key after Revocation

After a certificate has been declared invalid, no re-key is possible. A new certificate has to be requested. The procedure according to chapter 3.2 applies.

3.4 Identification and Authentication for Revocation Request

Requests for revocation are authorized by the authentication means submitted during registration.

Invalidation by natural persons:

- Personal authentication means of the applicant.

Invalidation by legal persons.

- Personal mobile phone number of a representative of the applicant or
- SSL/TLS client certificate provided by the applicant as a legitimate means of authentication as a method for releasing remote signatures.

If the certificate holder has lost his means of authentication, he can also submit the revocation by sending a signed request for revocation, stating the serial number of the certificate by mail (address see section 1.5). To verify the identity, the subscriber is called back via the company centre during business hours, and the revocation is only carried out afterwards

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

Certificate applications can be submitted by natural or legal persons at Swisscom ITSF registration authorities (especially RA partners). The procedure according to chapter 3.2 applies.

4.2 Certificate Application Processing

The registration authority conducts the identification and authentication of an applicant in accordance with the procedures set out in section 3.2 and then notifies the applicant of the date on which his application can be validated. After successful validation by the registration office, the certificate application will be further processed by Swisscom ITSF:

- The use by natural persons is released immediately after confirmation of the registration authority.
- The use by legal persons is released within 10 working days after confirmation of the registration authority.

4.3 Certificate Issuance

4.3.1 Certificate Issuance for Natural Persons

Certificates and cryptographic keys for natural persons are created immediately before use in an access protected environment of Swisscom ITSF and are kept there for the creation of the signature. The subscriber can use signatures of the applied certificate class by confirmation its authentication means registered during identification (signature creation data).

4.3.2 Certificate Issuance for Legal Persons

The certificate issuance proceeds as follows:

- It is ensured that an HSM is used,
- a certificate of the requested class is issued by Swisscom ITSF,
- the certificate and the associated cryptographic key are stored in the Trust Centre,
- the SSL/TLS-Client certificate that was supplied during the identification process is linked to the associated user account so that the creation of seals via remote access is only possible through the possession of the associated private key (signature creation data),
- the subscriber is informed of the provision.

4.4 Certificate Acceptance

By using the certificate or by authorizing the creation of the signature in the case of remote signatures, the subscriber confirms the correctness of the data deposited at the registration office and accepts the certificate linked to the signature.

4.5 Key Pair and Certificate Usage

4.5.1 Use of Keys and Certificates by the Subscriber

Through the use of the certificate, the subscriber assures all stakeholders as per chapter 1.3 that:

- all the details and declarations of the subscriber relating to the information contained in the certificate correspond to the truth,
- the signature creation data (for example, PIN or password) for the release of the signature or seal generation are dealt with in accordance with the Swisscom ITSF Terms and Conditions of Use,
- the certificate is used exclusively in accordance with this CP / CPS.

The subscriber with his own HSM also assures that

- an appropriate understanding of the use and use of certificates exists,
- the private key is kept protected,
- no unauthorized person is granted access to the private key,
- he immediately abandons the creation of further signatures if the details of the certificate are no longer correct or the private key is lost, stolen, or otherwise might have come to knowledge of third parties (compromise).

4.5.2 Use of a Subscriber's Public Key and Certificate

Any person who, as a relying party (see chapter 1.3), verifies an electronic signature based on a certificate as per this CP / CPS, is required to

- have a basic understanding of the application and usage of certificates;

- use appropriate components and procedures for the signature verification;
- check the appropriate CRL or OCSP response before relying on the information in a certificate.

4.6 Certificate Renewal

Swisscom ITSF does not issue new certificates based on an already used key (certificate renewal).

4.7 Certificate Re-Key

A subscriber may submit a request for a new certificate with a new key pair (re-key) to a registration authority without justification.

Swisscom ITSF will issue a new certificate using the already validated data, provided that the subscriber still has the same authentication means. The subscriber has to confirm that the information submitted during identification (see section 3.2) is still valid.

The CP / CPS and Terms and Conditions of Use valid at the time of the certificate renewal applies.

4.8 Certificate Modification

Swisscom does not make any changes to already issued certificates.

4.9 Certificate Revocation and Suspension

4.9.1 No Revocation with a short Validity

For certificates whose validity period is less than 1 hour no revocation is made.

4.9.2 Circumstances for Revocation

Subscribers have to request revocation of their certificates immediately if

- the private key or other signature creation data for the creation of signatures or seals has been lost, stolen, disclosed or otherwise compromised or abused;
- the affected certificate is no longer required;
- there is a risk of misuse of the certificate;
- the information in the certificate is incorrect.

Certificates must be revoked by Swisscom ITSF if:

- the subscriber (natural or legal person) requests its revocation or
- Swisscom ITSF becomes aware of at least one of the following reasons:
    - knowledge of the death of the subscriber or any other change of certified attributes in the certificate;
    - the private key of the subscriber or that of Swisscom ITSF for an issuing CA has been lost, stolen, disclosed or otherwise compromised or abused;
    - the certificate was obtained based on wrong information;
    - Swisscom ITSF ceases its activities in whole or in part and its directory and revocation services are not taken over by another TSP;
    - the supervisory body orders the suspension of the certificate in accordance with Article 6 of the SVG;
    - the subscriber does not comply with this CP / CPS;
    - the responsible registration authority does not comply with this CP / CPS;

- the subscriber fails to comply with his obligation to pay the fees even after repeated requests;
- if the certificate does not or no longer complies with the specifications of the underlying CP/CPS
- or the crypto-algorithm or key lengths used are no longer considered secure
- one of the reasons for the revocation is provided by the subscriber.

4.9.3 Who can request the Revocation

The following entities may request revocation of a certificate:

- Each subscriber may require the registration authority, who has issued his certificate, to revoke his certificate;
- Swisscom ITSF may revoke any certificate issued within the PKI at its sole discretion;
- A registration authority may request revocation of certificates that it requested to be issued;
- the supervisory body may order the suspension of a certificate.

4.9.4 Procedure of a Revocation

The identification and authentication with a revocation shall be in accordance with section 3.3. If the prerequisites for the revocation of a certificate are met, the certificate will be revoked according to the following process. The due dates are described in section 4.9.5.

The process is as follows:

- The subscriber submits the application for the revocation to the registration authority which conducted the identification process.
- The registration authority verifies the identity of the applicant and the reasons for the revocation.
- If a valid reason for revocation exists, the certificate is revoked by Swisscom ITSF.
- Swisscom ITSF updates the revocation information (OCSP) with the revoked certificates.
- Swisscom ITSF confirms the subscriber the revocation of the certificate.

The revocation of a certificate cannot be undone.

4.9.5 Time Limits

The subscriber shall promptly notify the registration authority that carried out the identification process and promptly invalidate his / her own certificate if there are reasons for invalidity according to chapter 4.9.2.

On business days, the registration authorities and Swisscom ITSF shall file a request for revocation of a certificate within 3 hours of receipt of the application. Outside of this period the revocation of a certificate will be triggered no later than six hours after receipt of the application.

4.9.6 CRL

The CRL of the Root CAs is updated as needed, but at least once a year (frequency). After a change, a new CRL is published within a maximum of 12 hours (latency).

The URL under which the associated revocation list or OCSP is published is listed in the certificate.

The status information is available in the directory service for at least 35 years beyond the duration of the certificate.

Certificates of the class "Diamant" once included in the CRL will not be removed from the CRL.

4.9.7 Suspension

Swisscom ITSF does not suspend (interrupt) certificates.

4.10 Certificate Status Service

Swisscom ITSF provides a CRL for the Root CAs and an OCSP service for the Issuing CAs and the TSS CA, which can be used to check the status (especially the validity) of all issued certificates. Details on availability are given in chapter2.1.

The data in OCSP is updated immediately after each change.

4.11 Termination of the Contract by the Subscriber

The duration of the contractual relationship results from the certificate validity period specified in the certificate.

4.12 Key Escrow and Recovery

Swisscom ITSF does not offer key escrow and recovery.

Swisscom ITSF ensures that no copies of signature keys are created and that the private signature keys cannot be exported from the HSM.

When an HSM is used, a backup can be generated using special methods from the HSM manufacturer, which can only be restored on a defined HSM.

5 Physical, Procedural and Personnel Security Controls

Some guidelines, such as the role concept or the access policy, are available in separate documents, which are not published, but which can be requested at Swisscom ITSF for review.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

The PKI systems of Swisscom ITSF are located in Trust Centres. The important components are redundant and are located in two separate data centres of Swisscom (Switzerland) Ltd. in Switzerland.

The Trust Centres provide adequate protection and infrastructure protection measures and comply with legal requirements.

5.1.2 Physical Access

The Trust Centres are secured by suitable technical and infrastructural measures so that only employees who have a role within Swisscoms PKI organization are authorized. Access to the Trust Centres is protected by access systems.

5.1.3 Power and Air Conditioning

The data centres of Swisscom have an uninterruptible power supply (no-break). In the event of a power failure, electricity is produced by an emergency power unit.

In the Trust Centres redundant air conditioning systems ensure a suitable room temperature and humidity.

5.1.4 Water Exposures

The server rooms for the technical infrastructure have adequate protection against water damage.

5.1.5 Fire Prevention and Protection

There are fire protection regulations. In particular, the Trust Centres have a sufficient number of fire alarm systems and hand-held fire extinguishers.

5.1.6 Media Storage

Data storage devices are kept in locked rooms or cabinets. If data storage devices with sensitive data are not located in a Swisscom data center, they are kept in a vault.

5.1.7 Waste Disposal

All data on electronic data storage devices or paper are destroyed in a professional manner and then disposed of.

5.1.8 External Backup

The backups of the systems are stored in two different Swisscom data centers.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted roles must be taken over by persons who are subject to regular review. Such persons may be Swisscom ITSF employees or contractors. They have access to the systems of the Swisscom PKI and carry out activities which can have a significant effect on:

- Validation of information in certificate applications
- The acceptance, rejection or other processing of certificate applications
- Revocation or enrolment information
- Issuing or revoking of certificates
- the handling of the information or inquiries of the certificate applicant

Reliable persons include, but are not limited to:

- Administrators of cryptographic systems
- System administrators
- Engineers
- Information security officer
- responsible managers

The roles and responsibilities of people in trusted roles are distributed in such a way that a person cannot act alone, thus circumventing security measures and undermining the trustworthiness of PKI or TSA operations.

The assignment of trusted roles to persons is reviewed annually.

5.2.2 Number of Employees required per Task

Cryptographic devices such as HSM and CA servers are subject to special authentication procedures. For all accesses to these systems, the "dual-control principle" is enforced by technical or operational means (e.g. by using different PED-keys).

5.2.3 Identification and Authentication Requirements

The identification and authentication of the roles is described in the [Role Concept] of the Swisscom PKI. The technical access to the individual IT systems is realized by strong authentication or user ID and password.

5.2.4 Separation of Duties

The [Role Concept] stipulates a separation of the tasks to prevent the accumulation of incompatible roles on a person and thus to prevent conflicts of interest, to enforce the dual-control principle and to prevent harming behaviour.

5.3 Personnel Security Controls

5.3.1 Requirements for Employees

The employees of Swisscom, who are responsible for the operation of the platform or the monitoring, fulfil the legal requirements, in particular with regards to expertise, reliability, experience and qualifications.

In addition to a general education in the field of information technology, the employees have the appropriate expertise in the areas of:

- Computer general,
- Security technology, cryptography, electronic signature and PKI,
- technical standards, in particular evaluation standards,
- Hardware and software,
- rules on the safety and protection of personal data,
- Application of administrative and management procedures.

5.3.2 Background Checks

All employees with access to the Swisscom PKI have to provide (updated every three years):

- extract from the criminal record
- extract from the debt collection register

5.3.3 Training Requirements

Only qualified employees are employed in the operations teams of the Swisscom PKI. In addition, regular training for all employees of the organization is conducted by competent persons.

An employee receives an authorization to carry out a specific role only after proof of the necessary specialist customer.

Training courses are conducted, in particular with the introduction of new guidelines, IT systems and security engineering.

5.3.4 Sanctions for Unauthorized Actions

Unauthorized actions that endanger the security of the IT systems of the Swisscom PKI or violate data protection regulations are subject to disciplinary action.

5.3.5 Documentation to be supplied to Personnel

Swisscom PKI employees have access to course material, operating documents and procedural instructions on the Swisscom Intranet.

5.4 Audit Logging Procedures

5.4.1 Recorded Events

The following events are logged:

- Server-related events such as access attempts, system start-up and shutdown, system crashes, hardware errors, and software and configuration changes
- All activities on the CAs, such as the signing and revocation of certificates, CRL generation, etc.
- Installation and deactivation of cryptographic components
- Changes to the CP / CPS
- Access to the server rooms, technical alarms and intrusion alarms

Each logged event is time stamped and the person or process executing is specified.

5.4.2 Protection of Audit Logs

The log data is transferred to a central log server and protected against access, deletion and manipulation.

5.5 Archiving

5.5.1 Archived Data

All data relevant to the certification process are archived:

- Certificate applications (including supporting documents)
- Applications for revocation
- all events related to the life cycle of the keys managed or issued by Swisscom

Further, following data are archived:

- Contracts
- Activity journal of the Swisscom PKI

5.5.2 Retention period for Archived Data

The retention period in connection with certificates of the class "Diamant" shall be at least 35 years after the expiry of the validity of the certificates. In connection with certificates of the class "Saphir", at least 7 years after the expiry of the validity of the certificate.

5.5.3 Protection of an Archive

It is ensured by suitable measures that the data can neither be read or copied unauthorized, nor altered or deleted.

The ISO can authorize the retrieval and verification of the archived data.

5.6 Key Change-Over

When the keys of a CA or TSU need to be replaced, a new certificate is created and published as per chapter 2.2. If the key change over affects a root CA, additionally a new certificate is signed with the old key and published.

If a key of a CA has been compromised, the rules in chapter 5.7.3 apply.

5.7 Compromise and Disaster Recovery

5.7.1 Recovery Procedures in the Event of Compromise or Disaster

The procedures for handling security incidents and compromise of the private keys of a CA are documented. These procedures are known to the roles involved and are executed as required.

5.7.2 Recovery of IT-Systems

Swisscom ITSF applies comprehensive and effective procedures for the detection and treatment of incidents and weaknesses.

5.7.3 Compromise of the Private Key of a CA

If the private key of a CA has been compromised or if there is a reasonable suspicion of compromising, the following measures are taken:

- Revocation of the affected CA certificate as well as of all remaining valid certificates issued by this CA
- Immediate information to all certificate holders affected
- Revocation of further CA certificates for which the same reasons for compromise exist
- Information to the appropriate supervisory body
- The incident, its impact and the revocation information are published on the website (see section 2.1)
- Revocation of other CA certificates for which the same conditions of use and vulnerabilities exist (e.g. keys located in the same cryptographic device or generated under the same general conditions).

Subsequent to an investigation of the incident, new CA keys are generated and a new CA certificate is issued, considering the reasons for the compromise.

5.7.4 Business Continuity following a Disaster

A resumption of the certification service after a disaster or after a compromise is part of the emergency planning and can take place if the security of the certification service is ensured.

5.8 Business Termination

When the certification services are terminated, the following measures are taken:

- notification to the supervisory body, at least three weeks before business termination;
- If the supervisory body determines that the revocation of the still valid certificates is not permissible, Swisscom ITSF hands over all necessary media and information to the Federation;
- Otherwise revocation of all certificates still valid and impacted by the termination and transfer of the certificate database to another qualified TSP;
- The subscribers and the organizations issuing seals are immediately informed about the cessation of the business as well as of the revocation, transfer or continuation;
- transfer of the final Certificate Revocation List (CRL), the transaction journal and related documents to the TSP designated by the supervisory body;
- Secure destruction of all private keys of the affected CAs of the Swisscom PKI.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The key pairs of the root CA are generated and stored on a dedicated HSM. The IT system that contains the root CA is not connected to a network. The root CA and the associated HSM are located in the high-security area of the Trust Centre. The procedure for generating root CA keys is monitored by an independent auditor.

The key pairs of the issuing CAs and TSS CA are generated and stored in a separate HSM.

The key pairs of "Diamant" and "Saphir" certificates are also created and stored in an HSM and meet the requirements of [ETSI EN 319 411-2]. The HSM fulfils the requirements of the assessment level EAL 4+.

The HSMs used are at least "FIPS 140-2 Level 3" compliant. The HSMs are stored in such a way that the dual-control principle with key generation is enforced by organizational measures. The creation of CA keys is documented.

6.1.2 Provision of the Private Key to the Subscriber

Key pairs for certificates of the classes "Diamant" and "Saphir" are generated exclusively within an HSM and will be managed according to the requirements of the HSM in order to fill the EAL4+ standard. If the subscriber holds the key pair on a separate HSM, the HSM or the certificate in combination with the key pair for use on his HSM is handed over to him in an appropriate manner.

6.1.3 Provision of the Public CA Keys

All Swisscom PKI participants can access the public signature key (public key) of the Swisscom Root-CA and the issuing CAs via the directory service (see chapter 2.2).

6.1.4 Algorithms and Key Lengths

The cryptographic algorithms used, and their key lengths are based on the publications of the ETSI and are at least:

Root CA 2 (OID 2.16.756.1.83.10)

- At least RSA 4096 SHA-256 for the CA 2 root key
- At least RSA 2048 SHA-256 for the subordinate CAs (Level 1)
- At least RSA 2048 SHA-256 for end user certificates and certificates of the TSUs

Root CA 4 (OID 2.16.756.1.83.30.4.0)

- RSA 8192 SHA256WithRSAandMGF1 for the CA 4 root key
- RSA 4096 SHA256WithRSAandMGF1 for the CAs of the next level (Level 1) and the TSS CA
- RSA 3072 SHA-256 for end user certificates and certificates of the TSUs

Further details (such as algorithms and duration of use) are defined in the [Addendum EU] Profiles of Certificates, Revocation Lists and Online Status Queries.

6.1.5 Public Key Parameters and Quality Assurance

The CA certificates and the end-entity certificates of the classes "Diamant" and "Saphir" are issued based on keys conforming to the latest version of [ETSI TS 119 312].

In addition, the parameters of the "Diamant" certificates also meet the requirements of [ETSI EN 319 411-2].

6.1.6 Key Usage and Restrictions

The purpose of the key usage and any restrictions are set in the corresponding X.509 v3 field (keyUsage) (see [Addendum EU] to this CP / CPS, chapter 2).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Throughout the entire life cycle (including delivery and storage), the HSM modules are protected from unauthorized access by technical and organizational measures.

6.2.1 Standard of the Cryptographic Modules

The HSM modules used meet the requirements of the [eIDAS-VO] and are at least FIPS 140-2 Level 3 compliant.

The certification status of the HSM modules used is monitored throughout their life cycle. In the event of a change in the certification status, Swisscom ITSF will conduct an impact analysis and subsequently determine the necessary measures.

6.2.2 Splitting of Private Keys

Splitting of the private keys of the Swisscom Root-CA and the issuing CAs is not done.

6.2.3 Escrow of Private Keys

Private keys from subscribers are not stored.

6.2.4 Backup of Private Keys

Copies of the key pairs of the Root CA and Issuing CAs are made and kept on an HSM, which is stored in a safe. The same prerequisites and security measures apply to the backup system as for the productive system.

6.2.5 Archiving of Private Keys

Private keys of Root CA, issuing CAs or subscribers are not archived by Swisscom.

6.2.6 Creation and storage of private keys

The private keys of Root CA, Issuing CAs, or subscribers are created in HSMs solely and managed according to the requirements of the HSM in order to fulfil the EAL4+ trust level.

6.2.7 Activation of Private Keys

Two different PED-keys, which are owned by two different key holders, are used to activate the private keys of the CAs. Thus, the dual-control principle is technically ensured.

For advanced and qualified signatures and seals, the private key is activated by means of the signature creation data registered by Swisscom ITSF during the identification (chapter 3.2).

6.2.8 De-activation of Private Keys

The private keys of the CAs are deactivated by terminating the connection between HSM and the management software.

With advanced and qualified signatures, de-deactivation of private key is realized by interruption of the connection between HSM and the signature application.

The private keys for use for advanced and qualified seals are deactivated by terminating the connection between HSM and the signature software.

6.2.9 Destruction of private keys

When the private keys of the root CA or the subordinate issuing CAs and TSS CA are destroyed, the dual-control principle is used. The procedure is logged.

The private keys for use for advanced and qualified signatures are automatically deleted after end of the validity period of a certificate of in case of revocation.

The private keys for use for advanced and qualified seals are destroyed when the certificate is deleted (for example, after termination or expiration).

6.2.10 Quality of the Cryptographic Modules

Swisscom ITSF uses suitable hard- and software-based key generators to ensure the quality of the key material.

6.3 Other Aspects of Key Pair Management

6.3.1 Archiving of Public Keys

Public keys are archived in both directory service and media.

6.3.2 Validity of certificates and Key Pairs

The certificates issued by the Root CA and Issuing CAs have the following validity periods:

- Certificate of the Root CA for a maximum of 20 years
- Certificates of issuing CAs incl. TSS CA for a maximum of 10 years
- Certificates of the classes "Diamant" and "Saphir" as well as the certificates of the TSU for a maximum of 3 years

The validity of the keys and certificates is variable and can be taken from the certificate.

6.4 Activation Data

For server signatures, the private keys of the subscribers remain in the HSM in the Trust Center. The subscriber authorizes the use of his private key via the activation data registered with Swisscom ITSF (e.g., mobile phone number).

6.4.1 Activation Data for Private Keys of Natural Persons

Activation data for the use of private keys must comply with the requirements of [CEN EN 419 241-1] at least level 1 (Sole Control Assurance Level 1).

Activation data for the use of private keys of the certificate class «Diamant» must comply with the requirements of [CEN EN 419 241-1] level 2 (Sole Control Assurance Level 2)

6.4.2 Activation Data for Private Keys of Legal Persons

The passwords for activating private keys for use for qualified seals according to chapter 6.2.7 must be at least 6 characters long. After 5 incorrect entries, the PIN or password is blocked.

The passwords for activating private keys for use for advanced seals according to chapter 6.2.7 must be at least 6 characters long.

6.4.3 Activation Data for Keys of CAs

The activation of the CA's keys in the HSM requires the participation of at least two authorized holders of a trustworthy role (according to chapter 5.2.1).

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

All computers, proxies and other components used at Swisscom PKI are subject to a risk analysis and protected according to their risk potential. For the CA and the directory service, a change auditing software is used, which places a hash value over the configuration files and thus can detect changes.

In addition, the following security measures are implemented:

- Restrictive access control
- User authentication and authorization is based on the "need-to-know" and "need-to-do" principles
- Perimeter protection: virus protection, use of firewall cascades and Web Application Firewall (WAF).
- Use of current software releases and timely installation of security-relevant software updates

6.5.2 Quality of the Security Measures

The security measures are periodically verified by an accredited conformity assessment body.

6.6 Life Cycle Security Controls

6.6.1 Software Development

Software (proprietary or third-party) can only be used once it has been accepted and released.

6.6.2 Security Management Controls

Security management covers the following aspects:

- Bi-annual audits (compliance audit by an accredited conformity assessment body)
- Regular evaluation and development of the security concept (annually)
- Checking the security during operation (see also chapter 5.4)
- Logging of all security related operations
- Collaboration with the Swisscom Computer Security Incident Response Team (CSIRT)
- Implementation of upgrades and patches
- Implementation of upgrades or patches on a productive system only after release on a test system.

6.7 Network Security Controls

The network of the PKI is divided into various security zones, each of which is protected by a firewall. All assets (devices, key material and information) are classified and placed in the security zone that corresponds to their classification.

The management network is separated from the data network.

Critical security incidents are immediately pursued and processed in cooperation with the Swisscom CSIRT if necessary.

6.8 Time Stamping

Swisscom runs an internal time service. For the time base, two different external time signals are correlated to ensure that the internal time is synchronized with the coordinated world time (UTC). The time base is also distributed to all Swisscom PKI servers via the Network Time Protocol (NTP).

Based on this internal time service, Swisscom provides a time service.

7 Profiles for certificates, Certificate Revocations Lists (CRL), and Online Status Queries

The certificate profiles, revocation lists (CRL) and online status queries (OCSP) comply with the standard X.509 v3. The certificate profiles and CRLs also comply with the specifications of [RFC 5280] and the OCSP queries comply with the specifications of [RFC 6960]. They are described in detail in [Addendum EU] to this CP / CPS.

8 Compliance Audit and other Assessment

8.1 Compliance

The services, processes and security controls are based on the following laws and regulations:

- These CP / CPS and associated documents such as the security concept, the roll concept, etc.
- Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC [eIDAS-VO], in the version of 29.01.2015
- Austrian Federal Law on electronic signatures and trust services for electronic transactions (Signature- and Trust Services Law - [SVG]) as of 01.07.2016
- Austrian Ordinance on electronic signatures and trust services for electronic transactions (Signature- and Trust Services Ordinance - [SVV]) as of 02.08.2016
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, version 2018-03
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, Version 2018-04
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, version 2018-04
- ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures, version 2020-06
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons, version 2020-07
- ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons, version 2020-07
- ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements, version 2020-04
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps, version 2016-03
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles, Version 2016-03
- CEN EN 419 241-1:2018, Systems Supporting Server Signing; Part 1: General System Security Requirements

8.2 Certification

Compliance with the requirements set out in chap. 8.1 has been audited and certified by the Telecom Control Commission as a supervisory body within the framework of the conformity assessment of Swisscom ITSF as a qualified Trusted Service Provider.

8.3 Frequency of Compliance Audit

Swisscom ITSF commissions a conformity assessment body at regular intervals of two years, as well as in the event of safety-relevant changes to the CP/CPS, to check compliance with the specifications in accordance with these CP/CPS. In addition, the supervisory body is authorized to carry out random checks

of the Swisscom ITSF (including registration authorities) at any time in accordance with art. 20 para 2 [eIDAS-VO].

8.4 Assessed Areas

The areas affected by an audit shall be defined by the responsible conformity assessment body. For risks that necessarily require a review, certain areas can be identified in advance.

8.5 Remediation

Any deficiencies identified are rectified in consultation with the supervisory body and Swisscom ITSF or the audited registration authority.

9 Framework provisions

9.1 Remuneration

The remuneration is agreed upon in the respective contracts with Swisscom ITSF (e.g. in the contract concluded between Swisscom ITSF and RA partner).

9.2 Liability insurance of Swisscom ITSF

Swisscom ITSF holds liability insurance with cover that is sufficient for the purposes of [eIDAS-VO].

9.3 Confidentiality of business information

9.3.1 Data that are to be treated as confidential

Information concerning participants referred to in chapter 1.3 that does not fall under chapter 9.3.2 is regarded as confidential information. This information includes inter alia business plans, information concerning business partners and any other information collected during the registration process.

9.3.2 Data that need not be treated as confidential

Information that is contained in certificates and the list of certificates that have been declared invalid is not regarded as confidential (e.g. elements of the DN).

9.3.3 Responsibility for upholding the confidential status of information

Swisscom ITSF is responsible for taking measures to uphold the confidential status of information. Data may only be processed in relation to the provision of the service and may only be disclosed to a third party that has been subjected to a contractual duty of confidentiality. RA partners that are able to disclose data to Swisscom ITSF during the course of the processing of the application for a certificate and to which Swisscom ITSF may in turn disclose the processed data will not be regarded as third parties. Documents may be viewed for auditing and control purposes in the presence of a Swisscom Information Security Officer.

9.4 Data protection

9.4.1 General

Swisscom ITSF only collects, stores, and processes data that are required in order to provide the services and to administer and manage the customer relationship, and specifically in order to ensure a high quality of service along with operational and infrastructure security and for billing purposes.

Swisscom ITSF uses Swisscom (Switzerland) Ltd, which is based in Switzerland, in order to provide trust services. Swisscom (Switzerland) Ltd operates the IT systems in order to provide the trust services and these systems are located in Switzerland. Digital certificates are therefore issued in Switzerland. The service therefore is to be qualified as data processing under contract in Switzerland by Swisscom (Switzerland) Ltd, which is carried out on the instructions of Swisscom ITSF. Swisscom ITSF has concluded the agreements required for this purpose under data protection law with Swisscom (Switzerland) Ltd, to which the signatories consent by accepting the Terms and Conditions of Use.

9.4.2 Responsible handling of personal data

Swisscom ITSF and its RA partners abide in particular by the following principles:

- Personal data may only be procured lawfully.
- Data may only be processed in good faith and processing must be proportionate.
- Personal data may only be processed for the purpose indicated when the data were acquired, that is apparent from the circumstances or that is specified by law.

9.4.3 Disclosure to courts and other authorities

The duties of disclosure and cooperation of Swisscom ITSF towards courts and other authorities are not affected by the terms of this CP/CPS and by specific contractual arrangements. Swisscom ITSF is in particular required to hand over data concerning signatories to the courts and other authorities in accordance with applicable legislation.

In particular, upon request by a court or another authority, Swisscom ITSF will carry out an analysis of the electronic signatures based on its certificates.

9.4.4 Other circumstances in which data may be disclosed to third parties

If the signatory uses a pseudonym in the certificate, Swisscom ITSF must transfer data concerning the identity of the signatory if it is credibly established that there is an overwhelmingly justified interest in establishing his or her identity pursuant to § 8(1), no. 4 and (3) of the Austrian Data Protection Act.

9.5 Copyright

Swisscom ITSF holds copyright over the following documents:

- the present CP/CPS;
- the associated Terms and Conditions of Use.

Swisscom ITSF grants the RA partners and the signatories the right to pass on the documents indicated without amendment to third parties. No further rights will be granted. In particular, the disclosure of amended versions and the transposition into other documents or publications is not permitted without the prior written approval of Swisscom ITSF.

9.6 Warranty

9.6.1 Warranty of Swisscom ITSF

Swisscom ITSF warrants that the information contained in the certificate is consistent with the information obtained during the authentication process in accordance with this document (chapter 3).

9.6.2 Warranty by other participants

Further warranties are regulated in the relevant contracts concluded with Swisscom ITSF.

RA partners must warrant in particular that they comply with the requirements imposed upon them in accordance with this document and the legislation applicable to signatures.

9.7 Liability

9.7.1 Liability of Swisscom ITSF

The liability of Swisscom ITSF for qualified trust services is determined in accordance with Article 13 [eIDAS-VO] and Article 11 of the Austrian Act on Signature and Trust Services. The present document provides information to signatories concerning the limitations associated with usage of the services, which limitations apply to third parties by virtue of the certificate and the liability limitations in the Terms and Conditions of Use. Swisscom ITSF thus bears no liability for losses arising out of any usage of the services beyond the extent of these limitations (Article 13(2) [eIDAS-VO]).

Swisscom ITSF certificates may contain a monetary upper limit of transactions for the certificate. If the signature was created based on a certificate with a monetary upper limit, Swisscom ITSF is not liable for any damage caused by a use of the services that exceeds these limits.

The upper limit is listed in the corresponding certificates according to specifications from [ETSI EN 319 412-5] in a specific certificate field `QcEuLimitValue` [Addendum EU].

The liability of Swisscom ITSF in relation to non-qualified trust services (e.g. between Swisscom ITSF and the RA partners) is determined in accordance with contractual agreements. Unless the contractual agreements specify otherwise regarding the issue of liability, Swisscom ITSF will bear liability as follows: In the event of a breach of contract, Swisscom ITSF will bear liability for demonstrable losses unless it can prove that it was not at fault. The liability of Swisscom ITSF for losses caused wilfully or through gross negligence is unlimited. Insofar as permitted by law, Swisscom ITSF will bear no liability for losses resulting from minor negligence.

9.7.2 Liability of other participants

The liability of the signatory is regulated in the Terms and Conditions of Use and is determined in accordance with the relevant applicable law.

The liability of the RA partner will be regulated in the contract concluded between Swisscom ITSF and the RA partner.

9.8 Effective date and revocation

9.8.1 Effective date

These CP/CPS will take effect upon publication by the Information Service of Swisscom (see chapter 2.2).

9.8.2 Revocation

This document will remain valid until:

- it is replaced by a new version; or
- the operation of the trust service of Swisscom ITSF is discontinued.

9.8.3 Consequences of revocation

If the validity period of a certificate has not yet expired upon revocation of these CP/CPS or at the time the new CP/CPS take effect, the new CP/CPS will apply from the time of notification (see chapter 9.8.4) for the remaining validity period.

If the holder does not accept the new CP/CPS, he/she must refrain from any further usage of the certificate. By virtue of any further usage of the certificate, the certificate holder will be deemed to have accepted the new CP/CPS.

9.8.4 Individual notifications and communication with certificate holders

Swisscom ITSF will use the contact data (e.g. mobile telephone number) provided upon registration to inform the certificate holder directly or via delegated Registration Authority of the entry into force of a new version of the CP/CPS or Terms and Conditions of Use, in the event that the validity period of the certificate has not yet expired.

9.8.5 Amendments to this document

Any amendments to these CP/CPS will be announced in consultation with the conformity assessment body.

The communication follows the description in section 9.8.4.

9.9 Resolution of disputes

In the event of any dispute the participants will endeavour to resolve the dispute amicably.

9.10 Applicable law and jurisdiction

All legal relations pertaining to the services of Swisscom ITSF falling under this document will be governed by the relevant provision set forth in the contracts (including in particular the contract concluded between Swisscom ITSF and the RA partner, and the contract concluded between Swisscom ITSF and the certificate holder).

If these contracts do not contain any provision to regulate the matter, the following will apply:

- Unless specified otherwise under mandatorily applicable law (e.g. the provisions of consumer protection law), all legal relations pertaining to the services of Swisscom ITSF falling under this document will be governed by Austrian law, to the exclusion of the rules on the conflict of laws under private international law and the United Convention on Contracts for the International Sale of Goods of 11 April 1980.
- Unless specified otherwise under mandatorily applicable law (e.g. the provisions of consumer protection law), jurisdiction will lie exclusively in Vienna, Austria.

9.11 Compliance with applicable law

All participants will comply with the laws and regulations applicable to them.

9.12 Language

The legally binding version of this document is the original version in German. It has also been translated into English.