Certificate Policy /
Certification Practice Statement (CP/CPS)

For the Certificate Classes

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

Version: 3.2

Date: April 18, 2018

Swisscom (Switzerland) Ltd.
Alte Tiefenaustrasse 6
3050 Bern

Document history

Version	Date	Changed by	Comments/nature of the change
3.2	18.04.2018	Kerstin Wagner	Synchronized with German version 3.2
3.2	18.04.2018	Governance Board	Approval

Referenced Documents

[ZertES]	SR 943.03: Federal Act on Electronic Signatures, ZertES
[VZertES]	SR 943.032: Ordinance on Certification Services in the area of Electronic Signatures, VZertES
[TAV]	SR 943.032.1, TAV: Technical and administrative provisions for certification services in the field of electronic signatures
[UIDG]	Federal Act on the Company Identification Number, UIDG
[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"
[CEN/TS 419 241]	Security Requirements for Trustworthy Systems supporting Server Signing
[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]	Addendum to the CP/CPS: profiles of the certificates, certificate revocation lists (CRL) and online status requests (OCSP)
[TOU]	Terms and Conditions of Usage
[Role Concept]	Role Concept SDCS
[Security Concept]	Security Concept SDCS
[Authority Seals]	Concept for seal for authorities / cooperation with the signature validator V2.0, federal IT control body (ISB)

Table of Contents

1 Introduction

This document (hereinafter "CP/CPS") sets out the Certificate Policy (CP) and the Certification Practice Statement (CPS) of Swisscom (Switzerland) Ltd. (hereinafter "Swisscom") for issuing certificates complying with the Swiss Federal Act on Electronic Signatures, [ZertES] and the related Ordinance on Certification Services in the area of Electronic Signatures, [VZertES].

As a Trust Service Provider (TSP) Swisscom operates a trust service issuing advanced, regulated and qualified certificates for use for advanced and qualified electronic signatures and advanced and regulated electronic seals as well the issuing of qualified time-stamps.

The present CP/CPS refers to different certificate classes, "Diamant" for regulated and qualified certificates and "Saphir" for advanced certificates. If not otherwise indicated all specifications in this document apply to both certificate classes.

1.1 Overview

The structure of this CP/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 Trust Service Providers:

- ETSI EN 319 411-1 V1.1.1 (2016-02): 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 V2.1.1 (2016-02): 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 V1.1.1 (2016-03): Policy and Security Requirements for Trust Service Providers issuing Time-Stamps; [ETSI EN 319 421]

This English translation of the CP/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

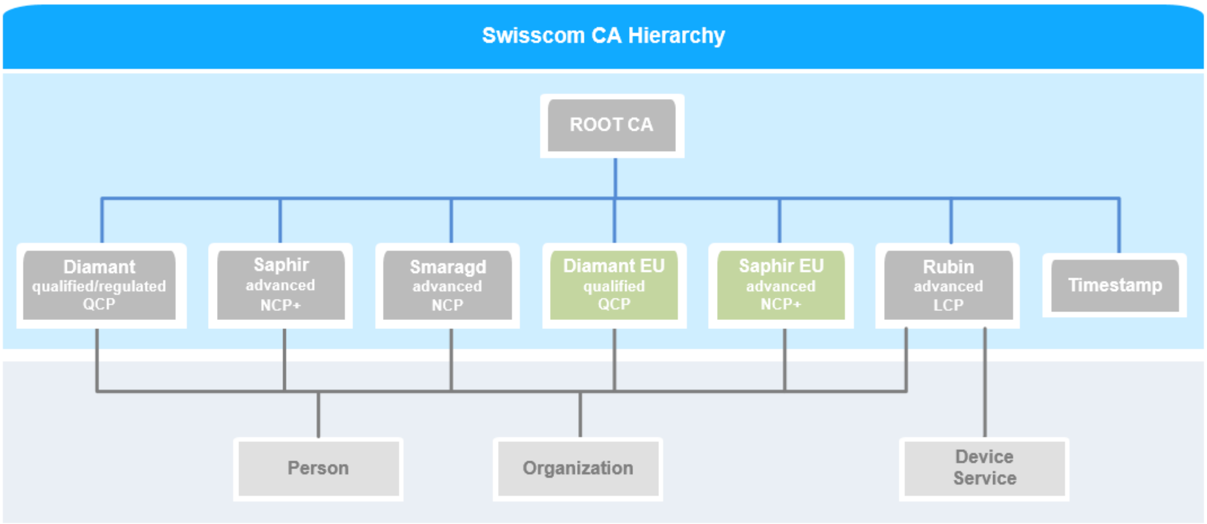
Title:	Swisscom Digital Certificate Services - Certificate Policy / Certification Practice Statement for the Certificate Classes „Diamant“ (qualified/regulated) and „Saphir“ (advanced)
Version:	3.2
Object Identifier:	2.16.756.1.83.11.0 - Diamant
	2.16.756.1.83.23.0 - Saphir

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 is structured hierarchically:



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

Swisscom IT Services Finance S.E., headquartered in Vienna, is responsible for the CAs labeled "EU". These CAs meet the very similar requirements to the CA of the same name without the suffix "EU", but comply with European and Austrian legislation and are subject to their own certificate directive.

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.

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

Diamant CA (legally regulated - QCP-n-qscd & QCP-l-qscd)

To issue certificates of the class "Diamant" to natural persons and organizations (such as legal entities and authorities). Meets the requirements of qualified certificates for electronic signatures for natural persons as set out in Art. 8 [ZertES] and for regulated electronic seals for legal entities as set out in art Art. 7 [ZertES] and uses a secure cryptographic device (QSCD).

Saphir CA (advanced – NCP+)

To issue certificates of the class "Saphir" to natural persons and organizations. Meets the requirements of certificates for advanced electronic signatures for natural persons and for electronic seals for legal entities and uses a secure cryptographic device (QSCD) as per [ETSI EN 319 411-1].

Smaragd CA (advanced – NCP)

To issue certificates of the class "Smaragd" to natural persons and organizations. Meets the definitions for electronic certificates of the category "Normalized Certificate Policy" (NCP) according to [ETSI EN 319 411-1].

Rubin CA (advanced – LCP)

To issue certificates of the class "Rubin" to natural persons and organizations. Meets the definitions for electronic certificates of the category "Lightweight Certificate Policy" (LCP) as per [ETSI EN 319 411-1].

Time-Stamping-CA

To issue time-stamps. Complies with the definition for qualified electronic timestamps as set out in Art. 2(j) [ZertES] and [ETSI EN 319 421].

1.3.2 Registration Authorities (RA)

The registration authorities identify and authenticate applicants, record and review applications for various certification services, archive the application documentation (inspected documents, authorizations, etc.) and forward the data to the certification authority. Swisscom may delegate the task of registration to third parties (hereinafter "RA partners"). RA partners are obliged by contract to comply with the processes defined in this document for registration, certificate issuance, revocation and archiving.

1.3.3 Subscriber

Subscribers are natural persons or organizations that can be uniquely identified by the name defined in the certificate. The subscriber is the person or organizations who holds the private key of their certificate and creates an electronic signature or seal based on this certificate.

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

1.3.4 Relying Parties

Relying parties are natural persons or organizations that use the certificates of this PKI (e.g. checking the validity of a signature) and have access to Swisscom's certification services.

1.3.5 Other Participants

Other participants can be natural persons or organizations 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 "Diamant" certificates issued under this CP/CPS can only be used as follows:

- Qualified certificates: for the creation of qualified electronic signatures by natural persons.

  If the certificates contain the label "Swisscom Digital Identification and Signing" in the subject (see Chapter 3.1), these can only be used in an environment closely related to the activity of the identifying financial intermediary. The certificates must not be used in other areas of activity.
- Regulated certificates: for creating regulated electronic seals by UID entities

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

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

The private keys of issuing CAs are used to sign the associated end user certificates, revocation lists, 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 shall not be liable for damages resulting from the use of the services beyond these restrictions.

1.5 Policy Administration

Publisher of this document:

Swisscom (Switzerland) Ltd.
Digital Certificate Services
P.O. Box
CH-8021 Zurich

Changes to this CP/CPS are approved by the Governance Board of Swisscom Digital Certificate Services.

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

1.6 Definitions and Acronyms

Term	Explanation
Advanced electronic seal	The advanced electronic seal is an advanced electronic signature based on an advanced certificate issued on an organization (such as a legal entity and authority).
Advanced electronic signature	The advanced electronic signature is an electronic signature that meets the following requirements: 1. it is exclusively assigned to the owner, 2. it enables the identification of the holder, 3. it is produced by means which the holder can keep under his or her sole control, 4. it is linked to the data to which it relates in such a way that any subsequent change in the data can be detected; (Art. 2(b) [ZertES])
Certificate Authority (CA), Issuing CA	Instance that issues digital certificates; this document refers to the device that issues and signs certificates; it is the central element of a PKI infrastructure.
Certificate Policy (CP)	Set of rules that prescribe the applicability of a certificate to a specific group of persons and/or a class of special applications with common security requirements.
Certificate status management	Service of the → Trust Service Provider (TSP)which enables users of a certificate to check whether it has been declared invalid.
Certification Practice Statement (CPS)	Information on the rules and guidelines effectively implemented by the TSP for issuing certificates. The CPS defines the equipment, methods and procedures used by the → Trust Service Providers (TSP) in accordance with its chosen certification guidelines.
Conformity Assessment Body	Body accredited under federal legislation for the certification and supervision of → Trust Service Providers (TSP). The Conformity Assessment Body is accredited by the Swiss → Supervisory Body
Digital Certificate	electronic certificate that links a signature verification key (private key) to the name of a person, organization or system.
Distribution of certificates	Service of the → Trust Service Provider (TSP), which consists of making the certificate available to the holder after it has been generated and - with the consent of the holder - to the users of the certificate.
Electronic signature creation device, Electronic seal creation device	Software/firmware or hardware configured to implement the signature key that the holder of the certificate uses to create an electronic signature or seal, e.g. a SmartCard or HSM.
Electronic signature/seal	Technical procedure for verifying the integrity of a document, an electronic message or the identity of the sender.
Hash	The hash function is a cryptographic checksum for a text to ensure its integrity. This procedure is used to reduce the computing effort involved in encrypting data using the public-key procedure. On the message that has a variable length, a hash function is applied that generates a checksum of fixed length, the hash value. This allows the integrity of a message to be determined beyond any doubt.
Holder of the certificate (Subscriber)	Natural person or organization who is the owner of the signature key assigned to the signature verification key listed in the certificate.
HSM (Hardware Security Module)	Device for the efficient and secure execution of cryptographic operations or applications. HSMs offer extensive functions for secure management of the device and the keys. As a rule, HSM are certified according to safety standards such as FIPS 140-2 or Common Criteria (CC).

Term	Explanation
Issuing of certificates	Service of the → Trust Service Providers (TSP); generation of a digital certificate on the basis of the name of the applicant for a certificate and any other attributes that are checked during registration.
Key pair	Signature keys and associated signature verification keys that are mathematically linked together by an asymmetric signature algorithm.
List of revoked certificates (CRL)	List signed by the CA that contains the serial numbers of all certificates that were declared invalid before they expired.
„On Demand“ creation and use of key material	"On demand" creation and use of key material (private and public keys and certificates) used for electronic signatures. The key pairs are generated and used in the secure environment of the → Trust Service Provider (TSP). The private key is deleted immediately after the signature is generated.
Qualified certificate	Digital certificate meeting the requirements of Art. 8 [ZertES].
Qualified electronic signature	The "qualified electronic signature" is an advanced electronic signature of a natural person created by a → secure signature creation device and based on a qualified certificate for electronic signatures. (Art. 2(e) [ZertES])
RDN-names, Relative Distinguished Name	Names of directory entries whose uniqueness refers to a particular entry and are the components of a directory name (Distinguished Name).
Registration	Service of the → Registration Authority, which consists of checking the identity and, if necessary, the attributes of each applicant of a certificate before their certificate is generated or the activation data (or password) is assigned to activate the use of the signature key.
Registration Authority	The Registration Authority is responsible for the proper → Registration of applicants. The validated applications are either forwarded to the certification authority (for creating → advanced or regulated electronic seals) or the applicant is activated in the signing application of the registration authority (→ "OnDemand" creation and use of key material).
Regulated electronic seal	The regulated electronic seal is an advanced electronic signature created using a secure seal creation unit and based on a regulated certificate issued on an organization Art. 2(d) [ZertES]
Revocation of the certificate	Service of the → Trust Service Provider (TSP), which cancels the validity of a certificate before its expiry.
Secure signature creation device	Signature creation device meeting the requirements of Art. 6 [ZertES].
Security Policy (SP)	A set of rules and guidelines developed on the basis of a risk assessment to reduce the likelihood of possible incidents (preventive measures) and to remedy the effects of such incidents (corrective measures) in order to protect the resources identified as worthy of protection by the → Trust Service Provider (TSP). The security strategy and policy can clearly define the overall security level to be achieved for an information system and especially for each element of the security architecture.
Signature key (private key)	Unique data such as codes or private cryptographic keys used by the owner to create an electronic signature or seal.
Signature verification key (public key)	Data such as codes or public cryptographic keys used to verify an electronic signature or seal.
Supervisory Body	An area of the State Secretariat for Economic Affairs (SECO), which performs supervisory tasks in Switzerland, including the accreditation of → Conformity Assessment Bodies.
Timestamp object recipient (Relying Party)	Recipient of a timestamp object that trusts this timestamp object.
Timestamp Service User (Subscriber)	Natural person who timestamps his own data or data of a legal person or organization using a timestamp service.

Term	Explanation
Time-stamping	Service of the → Trust Service Provider (TSP) which issues a certificate bearing the date, time and a qualified signature stating that certain digital data 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 timestamp service during the creation of signed timestamps.
Time-stamping token	Data object that links the representation of a fact with a certain point in time and thus provides proof that the fact existed before the point in time.
Time-stamping Unit	The IT infrastructure with which time stamp objects can be created. Only one private key exists on this unit for issuing timestamp objects.
Trust Centre	Specially protected room in which the infrastructure of the → Trust Service Provider (TSP) 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 effectively implemented by the time stamp service for issuing time stamp objects. The → Trust Service Provider (TSP) defines the equipment, methods, and procedures used by the timestamp provider to issue and manage timestamp objects.
UID unit	UID unit according to Art. 3 paragraph 1 (c) of the Federal Act of 18 June 2010 on the Company Identification Number (UIDG). Mostly: - legal persons - groups of persons without legal capacity (e.g. ordinary partnerships) - individual companies - certain administrative units of the Confederation, cantons and municipalities
User of the certificate (Relying Party)	Person or process who relies on the verified electronic signatures or seals when using this certificate.
UTC, coordinated Universal Time	Universal time scale based on seconds. UTC is defined in ITU-R recommendation TF.460.

1.7 Abbreviations

AIS	All-in Signing Service
CA	Certification Authority
CSIRT	Computer Security Incident Response Team
CN	Common Name, as part of the DN
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DIS	Digital Identification and Signing; video identification method
DN	Distinguished Name as per RFC 3739
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
ISO	Information Security Officer
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
Mobile ID	two factor authentication method based on SIM-cards
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OFCOM	Swiss Federal Office of Communications
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PDS	PKI Disclosure Statement
PED	PIN Entry Device
PIN	Personal Identification Number
QSCD	Qualified Secure Electronic Signature/Seal Creation Device, as per ISO/IEC 15408
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	Certificate renewal with new keys
SAS	Signature Activation Service; authentication method using a password and an additional One-Time-Password
SCD	Secure Electronic Signature/Seal Creation Device
TAV	Technical and administrative regulations on electronic signatures
TLS	Transport Layer Security
TSA	Time-stamping Authority
TSP	Trusted Service Provider
UIDG	Federal Act on the Company Identification Number
VZertES	Ordinance on Electronic Signatures
ZertES	Federal act on Electronic Signatures

2 Publications and Repository Responsibility

2.1 Repository Service

Swisscom publishes its CA certificates, revocation lists (CRL), CP/CPS documents and Terms and Conditions of Usage on the web.

The repository of the Swisscom trust services is located at: http://www.swissdigicert.ch

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 usage
- Certificates of the Root-and Issuing CAs
- Certificate revocation lists
- Information about the issued certificates, if requested by the certificate holders

Adaptations in these documents are communicated according to the specifications in chapter 1.5.

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): every 60 minutes
- 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 available publicly and free of charge.

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 or the registration authority is informed of an infringement of such rights, Swisscom may declare the certificate invalid.

3.1.1 Name Components Required for Natural Persons

The DN of natural persons must consist of country, display name and either first/last name or pseudonym and may be supplemented with optional elements according to 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.
Display 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* *GN/SN*	givenName (G oder GN)	Formal first name(s) of the subscriber	Exact reproduction of the contents of the corresponding field from the presented identity document.
	surname (SN)	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 a service used for identification or authorisation (like Mobile ID, SAS, DIS) • Character string according [ETSI EN 319 412-1-5] of "Natural person semantics identifier" • Definition used before Jan 1st, 2018 If a pseudonym is used, which ensures the uniqueness, the serialNumber can be omitted.

3.1.2 Name Components Required for Organizations

The DN of an organization must consist of country, common name, company (names) according to the entry in the commercial register and an identifier derived from the company identification number (UID or similar) and may be supplemented with optional elements according to 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.
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	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.

Element	X.520 attribute	Content	Description
Uniqueness	organization Identifier	String derived from the official register number of the organization	Character string according [ETSI EN 319 412-1-5] 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 only permitted for test certificates if they contain a generally comprehensible identification element such as mobile phone number or ID card number.

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:

1. 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:

i. 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);

ii. It is a connection of a telecommunication service provider, which is subject to the Swiss Telecommunications Law;

e. applications signed electronically by a certificate from a Trusted Service Provider.

2. The registration authority reviews the documents submitted and validates their compliance with the information contained in the application.
3. 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.
4. The registration authority checks the existence and correctness of the applicant's mobile phone number and registers the number as a legitimate authentication means for later adjustments of the user data and as a method for the release of remote signatures of Swisscom.
5. The applicant confirms his acknowledgement of the procedure described above and the acceptance of the Swisscom Terms and Conditions of Usage 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 in accordance with Art. 7 [VZertES].
2. The applicant must present a passport or an identity card recognized for entry into Switzerland in person;
3. 3. the documents submitted must be valid at the time of registration;
4. 4. the registration and use of the mobile telephone number must be carried out using a procedure corresponding to Level 2 (Sole Control Assurance Level 2) as described in [CEN/TS 419 241]. The procedure may only be used with Swisscom remote signatures upon presentation of such a certificate.

The certificate application, the proof of identity and the consent to the Terms and Conditions of Usage are archived for at least 11 Jahre after issuing of the last signature.

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 is still valid.

3.2.2 Identification for Applications by Organizations

The following procedural steps are applicable for the validation of applications by organizations 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 regards 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 UID register (or equivalent commercial register), or
   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 commercial 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 commercial register, authority register).
4. The registration authority verifies the presence and compliance with the technical minimum requirements of the TLS client certificate provided by the applicant as a legitimate authentication means as a method for the approval of remote signatures of the Swisscom.
5. The applicants confirm their acknowledgement of the described procedure above and the acceptance of the Swisscom Terms and Conditions of Usage for the relevant Certificate Class

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

1. The applicant's representative must be present in person or a procedure has to be used which has been approved by a conformity assessment body in accordance with Art. 7 [VZertES].
2. The applicant's representative shall submit:
   a. If the applicant is registered in the commercial register (or equivalent register): a current and certified extract from the commercial register (or equivalent register), or
   b. If the UID unit has not agreed to the publication of its data on the core characteristics in the UID register (Art. 11 para. 3 UIDG): a current and certified extract from the UID register, or
   c. If applicant's representative himself is not registered in the commercial register as the sole authorised signatory: a written power of attorney to submit an application for a certificate, issued by the managing body of the applicant (e.g. executive board or management) or by two persons registered in the commercial register as authorised signatories. Individual signatures are only accepted if the individual signature authorization is noted in the extract from the commercial register, or
   d. If the applicant is not registered in the commercial register (e.g. simple partnership, partly association): a written power of attorney to submit a certificate application, issued by the applicant's supreme body (e.g. board or managing director).

3. The applicant must describe how the private key of the TLS client certificate used for certificate use is physically and logically protected against theft and that access is blocked after several failed attempts.

The certificate application, the proof of representation and identity and the consent to the Terms and Conditions of Usage are kept for at least 11 years after the last seal has been issued.

If the applicant wishes to remain in possession of the private key himself, the applicant must additionally prove that both the key generation and the storage and use of the private key take place exclusively in a certified system in accordance with the requirements set out by FIPS 140-2 Level 3 or higher. To this end, the applicant must submit an appropriate certificate of the hardware used and a written confirmation from the Recognition Authority or a representative of Swisscom RA that the keys have been generated, stored and used in accordance with the regulations.

3.2.3 Identification for applications from administrative bodies (authorities)

Administrative bodies are identified in accordance with chapter 3.2.2.

The identification of Swiss administrative bodies can be specifically regulated as soon as the relevant basis ([Authority Seals]) is available.

3.2.4 Non-verified Information

All information that is included in the certificate is checked. In addition, no further information is checked.

3.2.5 Method for proving Possession of Private Key

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

If the applicants themselves want to remain in possession of the private key, they must

- submit a certificate request electronically signed with the associated private key, or
- submit a written confirmation from the recognition authority or a representative of Swisscom RA which allows conclusions to be drawn about 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 valid 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.

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 new certificate will be issued. A new certificate has to be requested (chapter 3.2).

3.4 Identification and Authentication for Revocation Request

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

Invalidation for natural persons:

- Personal mobile phone number of the applicant.

Invalidation for legal persons.

- Personal mobile phone number of a representative of the applicant.
- 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 revocation request by mail (address see section 1.5), stating the serial number of the certificate and the reason for revocation. To verify the identity, the subscriber is called back during business hours via the company headquarters, 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 persons or organizations to Swisscom registration offices (in particular to RA partners). The procedure set out in chapter 3.2 shall apply.

4.2 Certificate Application Processing

The registration authority identifies and authenticates an applicant in accordance with the procedures set out in section 3.2 and then informs the applicant of the date by which his application may be verified. After successful verification by the registration authority, the certificate application is processed further by Swisscom:

- Use by natural persons will be activated immediately after confirmation by the registration office.
- Usage by organizations will be activated within 10 working days after confirmation by 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 the Trust Center of Swisscom and are kept there for the creation of the signature. The subscriber can use signatures of the applied certificate class by confirmation on his mobile telephone registered during identification (signature creation data).

4.3.2 Certificate Issuance for Organizations

The certificate issuance proceeds as follows:

- It is ensured that an SCD is used,
- a certificate of the requested class is issued by Swisscom,
- the certificate and the associated cryptographic key are stored
  - in the Trust Center and the 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), or

  - in the customer's HSM after Swisscom has assured herself that the customer complies with the required specifications.
- 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 Terms and Conditions of Usage,
- the certificate is used exclusively in accordance with this CP/CPS.

The subscriber with his own SCD (e.g., HSM) also assures that

- there is an appropriate understanding of the application and use of certificates,
- 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

In reasonable exceptional cases Swisscom may issue a new certificate based on an already used key pair (certificate renewal), provided that the renewed certificate is intended for the same certificate holder. The renewed certificate must have a different serial number to distinguish it from the original certificate.

The identification of the certificate holder must meet the requirements of chapter 3.2.

The CP/CPS valid at the time of the certificate renewal applies.

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.

After positive authentication of the certificate holder in accordance with chapter 3.3, Swisscom will issue a new certificate using the data already verified, provided that the certificate holder still has the same means of authentication. The certificate holder must confirm that the information recorded during identification (see chapter 3.2) is still valid.

The CP/CPS valid at the time of the certificate re-key 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

Certificates whose validity period is shorter than the update interval of the CRL (see chapter 4.9.6) are not revoked.

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 if:

- the subscriber (natural person or organization) requests its revocation or
- Swisscom becomes knowledge 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 for an issuing CA has been lost, stolen, disclosed or otherwise compromised or abused;
    - the certificate was obtained based on wrong information;
    - Swisscom ceases its activities in whole or in part and its directory and revocation services are not taken over by another TSP;
    - 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;
    - any reason requiring revocation by the subscriber.

4.9.3 Who can request the Revocation

Certificates can only be declared invalid by Swisscom. Any certificate holder may request the registration authority that issued his certificate to invalidate a certificate issued for him, stating reasons.

4.9.4 Procedure of a Revocation

The identification and authentication with a revocation shall be in accordance with section 3.4. If the prerequisites for the revocation of a certificate are met, the certificate will be revoked immediately.

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.
- Swisscom publishes the updated CRL with the revoked certificates.
- Swisscom 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.

4.9.6 CRL

The CRL is regenerated every 60 minutes (frequency). In the case of a change, a new CRL is published within a maximum of 60 minutes (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 11 years beyond the duration of the certificate.

4.9.7 Suspension

Swisscom does not suspend (interrupt) certificates.

4.10 Certificate Status Service

Swisscom provides a CRL and an OCSP service, which can be used to check the status (especially the validity) of all issued certificates. Details on availability are given in chapter 2.2.

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 does not offer key escrow and recovery.

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

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 for review.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

The PKI systems of Swisscom are located in Trust Centres. The important components are redundant and are located in two separate data centres of Swisscom 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 the companies 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 interruption-free 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 centre, 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 one data centre's systems are kept in the other data centre and vice versa.

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 employees or contractors. They have access to the systems of the Swisscom PKI and carry out identity checks or cryptographic operations 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. 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:

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

5.3.3 Training Requirements

Only qualified employees are employed in Swisscom PKI's operational organisation. An employee only receives authorization to perform a specific role after proof of the necessary technical qualification.

Training is provided in particular for the introduction of new guidelines, IT systems and security technology. In addition, all Swisscom employees receive regular training (at least every 12 months) on new threats and current security practices.

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
- Access to the server rooms, technical alarms and intrusion alarms
- Changes to the CP/CPS

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)
- Consent to the Terms and Conditions of Usage
- 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 is at least 11 years after expiry of the validity of the certificates.

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 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 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
- Information to the appropriate supervisory body
- The incident and its impact are published on the website

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 and the conformity assessment body, at least 30 days before business termination;
- revocation of all certificates still valid and transfer of the certificate database to another certified TSP or OFCOM;
- 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 the private keys 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 are generated and stored in a separate HSM.

The key pairs of "Diamant" and "Saphir" certificates are also created and stored in HSM, which are located in the Trust Centres, and meet the requirements of [ETSI EN 319 411-2]

The HSM used are at least "FIPS 140-2 Level 3" compliant. The HSM 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 remain in the HSM in the Trust Centres. If the subscriber holds the key pair on a separate SCD, the SCD 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 TS 119 312] and are at least:

Root CA 2 (OID 2.16.756.1.83.10)

- RSA 4096 SHA-256 for the CA 2 root key
- RSA 2048 SHA-256 for the subordinate CAs (Level 1)
- RSA 2048 SHA-256 for end user certificates "Diamant", "Saphir" and timestamping

6.1.5 Public Key Parameters and Quality Assurance

The CA certificates and the 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 meet the requirements of the [TAV], chapter 2.3.3 as well as 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] 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 Art. 6 [ZertES] 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 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, and subscribers are created and stored in HSMs solely.

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 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-activation of private key is not applicable since these private keys can only be used once and are then destroyed.

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 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 a single application.

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 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 storage 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 for a maximum of 10 years
- Certificates of the classes "Diamant" and "Saphir" 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 Centre. The subscriber authorizes the use of his private key via the activation data registered with Swisscom (e.g., mobile telephone number).

6.4.1 Activation Data for Private Keys of Natural Persons

The PIN or passwords for enabling private keys to use for advanced and qualified signatures must be at least 6 characters long. After 5 incorrect entries, the PIN or password is blocked.

6.4.2 Activation Data for Private Keys of Organizations

The private key activation passwords for advanced and regulated electronic 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 their risk potential is protected accordingly. 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:

- 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.

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 qualified time service according to the requirements set out in Art. 2(j) [ZertES].

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

The profiles of certificate, revocation lists (CRL) and online status queries (OCSP) correspond to the standard X.509 v3 and are described in detail in [Addendum] 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.
- Federal Act on Certification Services in the Field of Electronic Signatures and Other Applications of Digital Certificates (Federal Act on the Electronic Signature, [ZertES]), as of 1 January 2017

- Regulation on certification services in the field of electronic signatures and other applications of digital certificates (Regulation on electronic signatures,[VZertES]), as of 1 January 2017
- Technical and administrative regulations on certification services in the field of electronic signatures and other digital certificate applications ([TAV]), as of 1 January 2017
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [ETSI EN 319 401], V2.1.1 (2016-02)
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [ETSI EN 319 411-1], V1.1.1 (2016-02)
- 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 [ETSI EN 319 411-2], V2.1.1 (2016-02)
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps; [ETSI EN 319 421], V1.1.1 (2016-03)
- CEN/TS 419 241:2014: Security Requirements for Trustworthy Systems Supporting Server Signing, [CEN/TS 419 241], 2014-06

8.2 Certification

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

8.3 Frequency of Compliance Audit

The conformity assessment body reviews Swisscom and the registries regularly as well as after any security-relevant changes to the CP/CPS.

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 conformity assessment body and Swisscom or the audited registration authority.

9 Framework Provisions

9.1 Remuneration

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

9.2 Liability insurance of Swisscom

Swisscom holds liability insurance with coverage that is sufficient for the purposes of [VZertES].

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 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 during the course of the processing of the application for a certificate and to which Swisscom 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 the Information Security Officer Swisscom Digital Certificate Services.

9.4 Data protection

9.4.1 General

Swisscom 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 (Schweiz) AG operates the IT systems for the provision of certification services and these systems are located in Switzerland. The digital certificates are thus issued in Switzerland.

9.4.2 Responsible handling of personal data

Swisscom 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 towards courts and other authorities are not affected by the terms of this CP/CPS and by specific contractual arrangements. Swisscom 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 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 must transmit the data on the identity of the certificate holder, provided that a predominant legitimate interest in determination of the identity is substantiated.

9.5 Copyright

Swisscom holds copyright over the following documents:

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

Swisscom 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.

Swisscom grants the Mozilla Foundation a right to use these CP/CPS in accordance with Creative Commons Licence "CC BY-ND 4.0" (Attribution-NoDerivatives 4.0 International) insofar as necessary in accordance with the "Mozilla Root Store Policy" of the Mozilla Foundation.

9.6 Warranty

9.6.1 Warranty of Swisscom

Swisscom 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.

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

If certification services are provided on the basis of advanced certificates (certificate class "Saphir") or areas other than the provision of certification services are affected (e.g. in the relationship between Swisscom and RA partners), Swisscom's liability is determined in accordance with contractual agreements.

Unless the contractual agreements specify otherwise regarding the issue of liability, Swisscom will bear liability as follows: In the event of a breach of contract, Swisscom will bear liability for demonstrable losses unless it can prove that it was not at fault. The liability of Swisscom for losses caused wilfully or through gross negligence is unlimited. Insofar as permitted by law, Swisscom will bear no liability for losses resulting from minor negligenceSwisscom's liability is determined in accordance with contractual agreements.

Unless the contractual agreements specify otherwise regarding the issue of liability, Swisscom will bear liability as follows: In the event of a breach of contract, Swisscom will bear liability for demonstrable losses unless it can prove that it was not at fault. The liability of Swisscom for losses caused wilfully or through gross negligence is unlimited. Insofar as permitted by law, Swisscom will bear no liability for losses resulting from minor negligence

Swisscom's liability for certification services on the basis of regulated and qualified certificates (certificate class "Diamant") is governed by Art. 17 [ZertES]. 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. Swisscom thus bears no liability for losses arising out of any usage of the services beyond the extent of these limitations.

9.7.2 Liability of other participants

The liability of the signatory is regulated in the Terms and Conditions of Usage 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 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 (see chapter 2.2) of Swisscom.

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 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 will use the mobile telephone number provided upon registration to inform the certificate holder (e.g. by SMS) of the entry into force of a new version of the CP/CPS, 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.

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 falling under this document will be governed by the relevant provision set forth in the contracts (including in particular the contract concluded between Swisscom and the RA partner, and the contract concluded between Swisscom 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 falling under this document will be governed by Swiss 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 Berne, Switzerland.

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.