Swisscom Digital Certificate Services

Certification Practice Statement (CPS)

For:

- Swisscom Root CA 2 (OID 2.16.756.1.83.10.0)
  Swisscom Root EV CA 2 (OID 2.16.756.1.83.21.0)
- Issuing CAs (Diamond, Sapphire, Ruby, Emerald, Quartz, Time-Stamping)

Abstract	Certification Practice Statement for certificates of Swisscom Digital Certificate Services, to issue digital certificates for the creation of qualified and advanced electronic signatures in accordance with the Swiss Federal Act on Electronic Signatures (ZertES), OelDI, GeBüV and CA/ Browser Forum.
Name	CPS_SDCS_2_16_756_1_83_2_1_en
Version	2.11
Classification	Public
OID of this CPS	2.16.756.1.83.2.1
CA Names	Swisscom Root CA 2, - Diamond CA 2, - Sapphire CA 2, - Ruby CA 2, Ruby CA 3 - Emerald CA 2, - Time-Stamping CA 2, Swisscom Root EV CA2 - Quartz CA2
CA Owner	Swisscom (Switzerland) Ltd.
Language	English (original version in German is legally binding)
CP Compliance start	1. Januar 2011 (Swisscom Root CA 2) 1. Januar 2012 (Swisscom Root EV CA 2)
Document approval	Governance Board of the Swisscom Digital Certificate Services

Document history

Version	Date	Responsible	Comments/type of revision
2.0	19. Jul 2011	Andreas Ziltener	Synchronized with German version 2.0
2.2	16.10.2012	Project Team	Updates for Mozilla Root Program
2.3	25.06.2013	Kerstin Wagner	Amend interval for CRL generation
2.4	02.07.2013	Hans Augstburger	Replace “Fixnet”
2.5	29.01.2014	Patrick Graber	Add certificate profile Saphirre for All-in Signing service, typo corrections
2.6	16.07.2014	Kerstin Wagner	Amend chapter 5, move the profiles to a dedicated document, add EV certificates, several corrections
2.7	02.10.2014	Patrick Graber	Add Rubin CA 3
2.8	23.12.2014	Patrick Graber	Add All-in Signing Service
2.9	15.01.2015	Stéphane Vaucher; Kerstin Wagner	General adaptations from a legally view (primarily on the new All-in Signing Service and, on the other hand, of general intelligibility of the document as a contract component)
2.10	10.11.2015	Kerstin Wagner	Amendments as per the German version
2.11	07.06.2016	Kerstin Wagner	Review and Update 2016; Move of the descriptions of the CAs of the 1st generation (CA 1) and SuisseID to a separate document.
2.11	24.06.2016	Governance Board	Approval

Referenced documents

[1] SR 943.03, ZertES: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Federal Act on Electronic Signatures)

[2] SR 943.032; VZertES: Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (Ordinance on Certification Services in the area of Electronic Signatures)

[3] SR 943.032.1, TAV: Technical and administrative provisions for certification services in the field of electronic signatures

[4] SR 641.201.511: Ordinance of the FDF on Electronically Transmitted Data and Information (OelDI, German: ElDI-V)

[5] SR 641.201.511.1 / Appendix: Technical and administrative guidelines for certification services in the field of electronically transmitted data and information (EIDI-V) related to the issuing of advanced certificates

[6] IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework"

[7] ETSI TS 101 456: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates

[8] [ETSI TS 102 023: Electronic Signatures and Infrastructures (ESI); Policy Requirements for time-stamping authorities

[9] Addendum to the CPS [13]: Description of the Profiles of Certificates, Certificate Revocation lists and Online status requests, provided by Swisscom Digital Certificate Services

[10] Guidelines for Extended Validation Certificates: Guidelines of the CA / Browser Forum for the issuance and management of Extended Validation certificates. (http://cabforum.org/EV_Certificate_Guidelines.pdf)

[11] Role Concept of the Swisscom Digital Certificate Services

[12] All-in Signing Service, https://www.swisscom.ch/signing-service

[13] Mobile ID, http://www.swisscom.com/mobile-id

[14] CEN/TS 419241: Security Requirements for Trustworthy Systems supporting Server Signing

Table of Contents

1 Introduction

This document describes the Certification Practice Statement (hereinafter referred to as CPS) and is a statement on the certification practices of Swisscom Digital Certificate Services (herein after referred to as SDCS), a service of Swisscom (Switzerland) Ltd.. SDCS issues qualified and advanced certificates in accordance with the Swiss Signatures Act, ZertES [1], the referenced technical and administrative implementation guidelines VZertES [2] and TAV [3]. The issuance and management of Extended Validation certificates is done in accordance to the guidelines of the CA/Browser Forum [10] and the issuance and management of qualified and advanced electronic signatures is done in accordance with the "Security Requirements for Trustworthy Systems supporting Server Signing" [14].

Associated with this document are the respective Certificate Policies (CP) of the respective certificate classes.

The aim of this CPS is to define processes for the issuing, administration and application of Swisscom Digital Certificate Services in such a way as to guarantee the secure, reliable and legally compliant operation of the offered certification services and use of the issued certificates.

The CPS also provides information on the practices of Swisscom Digital Certificate Services in relation to the issuing of certificates.

Certificates are used to assign a public cryptographic key to a person to electronically confirm the identity of the person or organisation. A certificate thus creates an association between a person or organisation and a cryptographic key.

When the term "qualified" is used in connection with electronic signatures and certificates it means that a service provider meets the requirements of the Swiss Signatures Act (ZertES [1]), the related Ordinance on Electronic Signatures (VZertES [2]) and the technical and administrative provisions for certification services in the field of electronic signatures (TAV [3]). Compliance with these provisions is assessed by a certification authority accredited by the Swiss Accreditation Service (SAS). Accredited certificate service providers (hereinafter referred to as CSP) are authorised to offer certificates for the creation and verification of "qualified" electronic signatures. The qualified signature can also be used for verifying origin (authenticity) and protecting against unauthorised modifications (integrity).

When the Swiss Signatures Act came into force on 1/1/2005, section 14, para. 2bis of the Swiss Code of Obligations (OR, SR 220) was introduced, in which the qualified electronic signature was accorded equal status as a person's hand-written signature, thus enabling declarations of intent (in particular for the conclusion of contracts) which normally require the written form as per article 12 pp. OR with a qualified electronic signature as far as there are not divergent legal or contractual form or delivery regulations..

A certificate is only as trustworthy as the procedure that is used to create it. Swisscom therefore divides certificates into "certificate classes". The higher the certificate class, the more extensive the identification checks involved before issuing a certificate. The certificates themselves contain information on the certificate class. To obtain the two highest classes of certificate, a person needs to go to a registration authority in person and provide official identification and possibly additional documents to prove all of the information to be included on the certificate.

1.1 Overview

This CPS was drawn up by Swisscom for the following purpose:

- To meet the requirements for a provider of qualified certificates in accordance with ZertES [1] and the associated implementation provisions [2] and [3];
- To meet the requirements for a provider of advanced certificates in accordance with OeIDI [4] and the associated implementation provisions [5];
- To meet the requirements for a CPS for EV SSL certificates in accordance with the guidelines of the CA / Browser Forum [10] for the issuance and management of EV SSL Certificates;
- To describe the services, roles, limitations and obligations related to the use of qualified certificates issued by Swisscom;
- To guarantee interoperability in the use of qualified certificates issued by Swisscom.

The structure of this CPS is based on the guidelines set out in RFC 3647 [6].

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

1.2 Document Identification

Identification

- Title: Swisscom Digital Certificate Services - Certification Practice Statement (CPS)
- Version: 2.11
- Object identifier (OID) for this CPS: 2.16.756.1.83.2.1
  This OID solely identifies the present document

The OID of Swisscom Digital Certificate Services is based on the RDN assigned by the OFCOM:

Position 1	**Position 2**	**Position 3**	**Position 4**	**Position 5**	**Meaning**
2					Joint ISO-CCITT Tree
	16				Country
		756			Switzerland
			1		Organisation names (RDN)
				83	Swisscom Digital Certificate Services

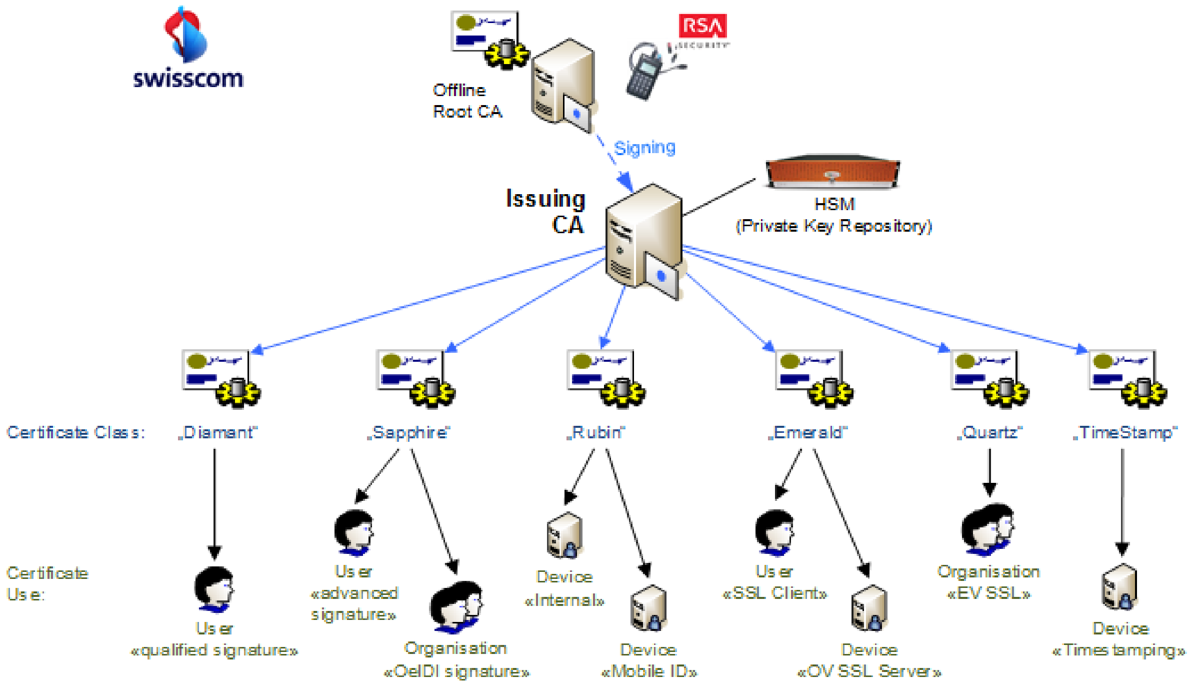
The positions 6-8 of the OID of Swisscom Digital Certificate Services refer to the respective CP / CPs document or to the respective CA

The OIDs assigned by OFCOM can be found on the Internet site of the OFCOM (http://www.eofcom.admin.ch/eofcom/public/searchEofcom_oid.do).

1.3 Swisscom Digital Certificate Services Participants

1.3.1 Certification Authorities (CAs)

The infrastructure of Swisscom Digital Certificate Services is built up hierarchically:



The operation of the infrastructure referred to here is done exclusively by Swisscom

1.3.1.1 Root CA

The public key of the root CA is stored in a self-signed certificate (Root Certificate). All participants of Swisscom Digital Certificate Services can access this certificate on the Internet site (http://www.swissdigicert.ch) to check the authenticity and validity of all certificates issued within Swisscom Digital Certificate Services under this root certificate.

The Swisscom root CA is not connected to any network and is only started when required. The root CA only issues certificates for certification bodies (CAs) which are part of the Swisscom Digital Certificate Services and which belong to the same certificate chain.

Fingerprints of the Root CAs

Name	Fingerprint Algorithmus	Fingerprint
Swisscom Root CA 2	sha1	77 47 4f c6 30 e4 0f 4c 47 64 3f 84 ba b8 c6 95 4a 8a 41 ec
Swisscom Root EV CA 2	sha1	e7 a1 90 29 d3 d5 52 dc 0d 0f c6 92 d3 ea 88 0d 15 2e 1a 6b

Subsequent to the Root CA the following certificate authorities (CA) of Swisscom Digital Certificate Services are operated:

1.3.1.2 Diamond CA (qualified)

To issue user certificates of class Diamond. Meets the requirements that ZertES puts for qualified certificates and qualified electronic signatures. The certificate owner or subscriber uses a secure signature creation device (SSCD). The key is used for creating qualified electronic signatures as per section 2, para. B ZertES. This level of certificate is only issued to natural persons, who nevertheless can represent legal entities. The certificate can only be used for signing.

1.3.1.3 Sapphire CA (advanced)

To issue user certificates of class Sapphire. Conforms to the definitions for advanced certificates as per section 2, para. B ZertES [1] and EIDI-V [8] and uses a secure signature creation device (SSCD). This type of certificate is used for creating signatures in cases where there is no provision for documents in paper form or for purposes which have been agreed by the parties. This type of certificate is issued for natural persons and organisations and can be used for signing and authentication.

1.3.1.4 Ruby CA

To issue certificates of class Ruby. These are soft certificates and the use of a secure signature creation device (SSCD) is not mandatory. This type of certificate is issued for internal devices (e.g. routers, access points, etc.) and Mobile ID and can be used for signing, encryption and authentication.

1.3.1.5 Emerald CA

To issue user and device certificates of class Emerald. These are soft certificates and the use of a secure signature creation device (SSCD) is not mandatory. This type of certificate is issued for natural persons, legal entities and devices and can be used for signing, encryption and authentication.

1.3.1.6 Time-Stamping CA

To issue certificates for the Time-Stamping Service. Conforms to the definitions set out in ZertES and ETSI 102 023 [6] for qualified certificates. Each Time-Stamping server has its own certificate. The private key for the issuing of time-stamping objects is created on a HSM.

1.3.1.7 Quartz CA

To issue server certificates of the class Quartz in line with the definitions of the CA / Browser Forum [14] for advanced certificates. These are soft certificates and the use of a secure-signature-creation device (SSCD) is not mandatory. This type of certificate is issued to organizations and can be used for authentication.

1.3.2 Registration Authorities (RA)

The business model of Swisscom is based on a registration authorities contractual partner model. Here Swisscom delegates its RA function to contractors (RA partners) and depending on the situation allows them to issue certificates themselves. According to the contract, it is up to the RA partner whether he wants to issue certificates only within his organization or to act as a "public" RA.

RA partners are obliged by the terms of a contract to comply with the processes defined by Swisscom for the registration, issuance and revocation of certificates. If the RA partner also wishes to issue qualified certificates it is incorporated in the authorisation process by a certification authority accredited by the Swiss Accreditation Service (SAS). If the RA partner only issues advanced certificates, it is audited by Swisscom at least once a year.

The Swisscom business model differentiates the following types of RA:

- **Swisscom RA**: To issue certificates for own use and underlying Enterprise-Registration Authorities.
- **Enterprise-RA**: (hereinafter E-RA) is a RA partner authorised to create and issue SSCDs and certificates within his organization directly.
- **Trusted Point of Sale** (hereinafter TPS) is a RA partner which, as a registration authority, receives and checks the details of certificate applications and then forwards them to a RA that is able to issue certificates for processing.

SSCDs for the “Diamond” and “Sapphire” certificate classes are personalised and distributed by a RA-partner or a central distribution point.

Employees of the registration authorities execute the identity check of applicants, with qualified certificates based on a contract that regulates the precise arrangements of the delegation of the RA activities as per section 8, para. 4 ZertES.

1.3.3 Subscribers

Certificate holders use their certificate to electronically sign or encrypt transactions, documents or communication (e.g. email) or to authenticate against a server or an application.

Before checking the identity and issuing a certificate, a subscriber is an applicant.

Issuing regulations depend on the certificate class and are governed by the respective CP.

1.3.4 Relying parties

Relying parties are individuals or companies that act in reliance on a certificate issued by a CSP. For the statements regarding the certificate checking please refer to the associated CPs.

1.3.5 Other participants

Other participants can be natural persons or legal entities who are involved in the certification or registration process as service providers. In the case of service providers legitimately acting on behalf of a subscriber or relying party, responsibility lies with the subscriber making the application.

1.4 Certificate usage

The exact scope of certificate usage is governed in section 1.4 of the respective CP.

1.5 Policy administration

1.5.1 Organisation and contact address

Policy administration (in the sense of definition and content management) is carried out on behalf of the Governance Board by

Swisscom (Switzerland) Ltd.
Digital Certificate Services
Müllerstrasse 16
8004 Zurich

The information security officer (ISO) drafts the CPS in collaboration with operations for the Swisscom internal consultation process.

1.5.2 Responsibility for the CPS

Overall responsibility and arbitrament for CPS content and compliance lies within the Swisscom Digital Certificate Services with the Governance Board. The Service Manager is responsible to the Governance Board for the correct provision of the services in accordance with the agreed CPS.

The Security Board analyses infringements of the CPS and reports to the Governance Board and the Service Manager.

1.6 Terms and keywords

Term	Explanation
Approval authority	Authority accredited in accordance with the accreditation law to certify and monitor providers of certification services. The approval authority is accredited in Switzerland by the Swiss Accreditation Service (SAS) as part of the Secretary of State for Economy (SECO)
CA/Browser Forum	Voluntary consortium of certification authorities, vendors of Internet browser software, operating systems, and other PKI-enabled applications that promulgates industry guidelines governing the issuance and management of X.509 certificates for use in Web sites and web applications
Certification authority (CA)	See “Certification Service Provider”
Certificate issuance	CSP service for making a generated certificate available to the subscriber and – if authorised by the subscriber – to other certificate users.
Certificate Practice Statement (CPS)	Statement on the rules and practices effectively applied by the CSP To issue certificates. The CPS defines the devices, the policy and the procedures used by the CSP in accordance with its chosen certification policy.
Certification policy (CP)	A set of rules indicating the applicability of a certificate for a specific user group and/or class of special uses with common security requirements.
Certificate revocation	CSP service for revoking a certificate before it is due to expire
Certificate revocation list (CRL)	A list signed by the CSP containing the serial numbers of all certificates which have been revoked before their validity has expired.
Certificate Service Provider (CSP)	Authority which confirms information in an electronic environment and issues digital certificates for this purpose.
Certificate status management	CSP service which enables certificate users to check whether a certificate has been revoked.
Digital certificate	Electronic certificate that associates a signature verification key with the name of a person.
Electronic or digital signature	Technical procedures to verify the authenticity of a document, an electronic message or the sender’s identity. The electronic signature and hand-written signature with the use of digital certificates as per section 14 para. 2bis OR are equivalent.
Generation of certificates	CSP service; generation of a digital certificate based on the name of the certificate applicant and his attributes, which are verified during registration.
Hash	The hash function is a cryptographic check sum applied to a text to ensure its integrity. The procedure is used to reduce the computing time when encrypting data in the public key process. A hash function is applied to a message or string of variable length to produce a check sum of fixed length - the hash value. This enables the integrity of a message to be positively determined.
Issuing CA	Issuing CAs are used to provide certificates to users, computers, and other services.

Term	Explanation
Key pair	Signature key and associated signature verification key which are mathematically linked by an asymmetrical 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 (SSCD) and deleted immediately after the signature they have been created for.**
Qualified electronic signature	Electronic signature meeting the following requirements (section 2 para.2 ZertES): 1. It is only assigned to the subscriber; 2. It enables the subscriber to be identified; 3. It is generated using methods which the subscriber can keep under his/her own control; 4. It is generated by a secure signature creation device in accordance with section 6, paragraphs 1 and 2 ZertES; 5. It is linked to data to which it is related in such a way that subsequent changes to the data can be detected; 6. It is based on a qualified certificate that is valid at the time of creation;
Qualified certificate	Digital certificate meeting the requirements of section 7 ZertES.
Registration	CSP service that verifies the identity and if necessary the attributes of each certificate applicant before his certificate is created or the activation data (or password) for activating the usage of the signature key is assigned.
Relying party	Person or process that relies on the verified electronic signatures when using a certificate.
Secure signature creation device (SSCD):	Device in accordance with section 6, para. 2 ZertES, configured for implementing the signature key that the subscriber uses to create an electronic signature.
Security policy (SP):	Set of rules and practices assembled on the basis of a risk analysis for reducing the probability of potential incidents (preventative measures) and for rectifying the effects of such incidents (corrective measures) in order to protect the resources of the electronic certification service provider that have been identified as requiring protection. The security strategy and policy are used to clearly define the target security level for an information system and especially for each element within the security architecture.
Signature verification key	Data such as codes or public cryptographic keys used for verifying an electronic signature.
Signature key	Unique data, such as codes or private cryptographic keys, used by the subscriber for creating an electronic signature.
Subscriber	Natural person who owns the signature key and who is assigned the signature verification key in the certificate.
Trust Center	Special protected room where the CSP systems are operated
Time stamp	CSP service for “stamping” a certificate with the date, time and qualified signature of the CSP to indicate a specific point of time in which specific digital data existed.

1.7 Abbreviations

AIS	All-in Signing Service
BCP	Business Continuity Plans
CA	Certification Authority
CN	Common name, as part of the DN
CP	Certification Policy
CPS	Certification Practice Statement
CSP	Certificate Service Provider
CRL	Certificate Revocation List
DN	Distinguished name in accordance with RFC 3739
FDF	Federal Department of Finance
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
HSM	Hardware Security Modules
ISO	Information Security Officer
LDAP	Lightweight Directory Access Protocol, repository service
OCSP	Online Certificate Status Protocol
OelDI	Provisions of the Federal Department of Finance (FDF) concerning electronically transmitted data and information (German: ElDI-V)
OID	Object Identifier
PED	PIN Entry Device
PIN	Personal Identification Number (for activating the signature key)
RA	Registration Authority (comprising the RA of Swisscom and LRA/TPS)
RDN	Relative Distinguished Name
Re-Key	Certificate renewal
SSCD	Secure Signature Creation Device in accordance with ETSI TS 101 456
SSL	Secure Socket Layer, security protocol
TSP	Time Stamping Profile
TPS	Trusted Point of Sales
TSA	Time-stamping Authorities
TAV	Technical and administrative provisions for certificate services with regard to electronic signatures
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (Ordinance on Electronic Signatures, VZertES)
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Federal Act on Electronic Signatures)

2 Publication and Repository Service

2.1 Repositories

Swisscom provides its root certificates, certificate revocation lists (CRL), CPs, CPS and terms of use on the Web.

The repository service of Swisscom Digital Certificate Services can be reached at the following address:

http://www.swissdigicert.ch

The online services to query root certificates, CRLs and OCSP responses are available around the clock with an availability of 99.9%.

2.2 Publication of certificate information

Swisscom Digital Certificate Services publishes the following information at https://www.swissdigicert.ch:

- Certificate of the Root and Issuing CAs of Swisscom: http://www.swissdigicert.ch/download_ca
- CPS and CP documents: http://www.swissdigicert.ch/download_docs
- CRLs: http://www.swissdigicert.ch/download_crl
- Terms of use: http://www.swissdigicert.ch/download_cond
- Status messages
- Contact information

2.3 Frequency of publication

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

- Certificates are published as soon as they are issued (if this comes into question for the affected certificates and if desired by the subscriber)
- Certificate revocation lists (CRL): every 2 hours
- Entries to the CRL are only added, never deleted
- Guidelines (CP/CPS): as required and following amendments
- Additional information: as required

2.4 Access controls on repositories

Unrestricted read-only access is available for certificate status information and public information in sections 2.1 and 2.2.

Certificates are public and can be retrieved by any users, provided the certificates are suitable for publication and were released by the subscriber.

Wildcard searches in the LDAP directory are limited.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

The name of each subscriber of Swisscom Digital Certificate Services must correspond to the following pattern:

- CN= Title, first name, middle name, surname,
  or name of the organisation
  or name of the device
  or pseudonym;
- C= Country code of the country, in which the subscriber's passport was issued (natural person) or the organisation is registered (legal entities) as per ISO Country Code DIN EN ISO 3166-1;
- If necessary, sequential number to ensure the uniqueness of the DN.

Based on these elements each certificate can be clearly identified with a legible indication of the certificate holder or the system.

Other attributes of the DN are possible. Mandatory and optional attributes that must or may be added to the DN are described in detail in the relevant CP, section 3.1.1. These descriptions also include a specification of the semantics and the test instructions.

3.1.2 Need for names to be meaningful

The name must uniquely identify the subscriber and be in a form that is meaningful to people. The following conventions also apply when assigning names:

- *Natural Persons*
  Name affixes can only be used if they are contained in an official ID with photograph, e.g.: "cn=Dr. Hans Peter Mustermann".
- *Legal entities and organisations*
  - *qualified*: Legal entities or organisations can only be represented by a natural person. When a certificate is issued to a natural person the corresponding names are entered in the CN=, O= and OU= fields as they appear in the official documentation submitted (e.g. commercial register extract). If the natural person who controls the signature key is not included in the certificate, the company name must be used as a pseudonym.
  - *advanced*: Advanced certificates for legal entities and organisations require a natural person for the administrative process. This does not have to be indicated in the certificate however. The CN field contains the name of the organization in accordance with the submitted official documents.
- *Persons or user groups*
  The "common name" of a person or user group should have a label of the type "GRP:", e.g.: "cn=GRP:Support" if it is not obvious that it is a natural person or legal entity.
- *Pseudonyms*
  The "common name" of a pseudonym begins with "PN:", e.g.: "cn=PN:Company Certificate".
- *Data processing systems*
  the "common name" of data processing system should always contain the fully qualified domain name, e.g.: "cn=www.swissdigicert.ch".

3.1.3 Anonymity / pseudonymity

The rules in section 3.1.2 apply. Swisscom and the RA partners offer pseudonym certificates in justified circumstances.

3.1.4 Rules for interpreting various name forms

The character code is printable string UTF-8 and IA5-String for E-Mail-Addresses.

3.1.5 Uniqueness of names

Rules regarding the uniqueness of names are set out in the respective CP.

3.1.6 Recognition, authentication and role of trademarks

The registration authority is not obliged to check the DN on compliance with rights of third parties. Only the certificate holder is responsible for such checks. If the registration authority is notified of an infringement of such rights, the certificate will be revoked.

3.2 Initial identity validation

Rules are set out in the respective CP.

3.2.1 Method for proving possession of private key

The signature key for qualified certificates is generated in the SSCD and, if necessary, delivered by secure means to an RA for personalisation. When using an HSM it must be ensured that the key pair was generated in the HSM and that the HSM is configured in such a way that the private key cannot be exported. This means that a procedure for checking the possession of the private key is not required for qualified certificates.

In the case of advanced certificates with SSCD (Sapphire), keys are also generated in the SSCD. A procedure for checking ownership of the private key is not necessary for this variant either.

All other certificate requests need to be submitted to the RA as signed PKCS#10 requests.

3.2.2 Authentication of a natural person

The basic procedures for checking the identity of a natural person are set out in the respective CP.

The highest standards of identity verification apply for the certificate class "Diamond" (qualified), and are based on section 8 ZertES und section 5 VZertES

3.2.3 Authentication of a legal person or other organization

The methods for the identity verification of a legal entity (association, foundation, corporation, partnership, limited liability company) or other organization of private law (particularly sole proprietorship, general partnership, limited partnership), can be found in the CP of the relevant certificate class.
Holder of a certificate of class "Diamond" (qualified) can only be a natural person. An application of a legal person or other organization for qualified certificates is therefore to be rejected. The authentication of a legal person or other organization for certificates of class "Diamond" is therefore excluded.

3.2.4 Authentication of a public body

The method for the identity verification of a public authority (authority, court, office management, public institution, etc.) of the CP, see the relevant certificate class.

Holder of a certificate of class "diamond" (qualified) can only be a natural person. An application of a public body for qualified certificates is therefore to be rejected. The authentication of a public body for certificates of class "diamond" is therefore excluded.

3.2.5 Applicants with a high risk

Swisscom considers coercive measures that are issued by the Swiss Confederation to enforce sanctions. In particular this means that

- certificate requests for natural and legal persons, groups and organizations, that are listed on the blacklist[1] published by SECO or on the blacklist[2] of the United Nations (UN),
- certificate requests from persons who request an attribute relating to the blacklist mentioned above

are rejected without giving any reason.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key requests

Rules are set out in section 3.3.1 of the respective CP.

3.3.2 Identification and authentication for re-key after revocation

Rules are set out in section 3.3.2 of in the respective CP.

3.4 Identification and authentication for revocation requests

Responsibility for revoking a certificate lies in principle with the registration authority that receives the application for the certificate. Certificates can be revoked in the following ways:

- In person at the registration authority giving details of the authorisation information or identity check in accordance with section 3.2.
- A signed revocation order with the details of the certificate is sent by post. The subscriber is called back to verify his identity.
- Phone call at the responsible RA giving details of the authorisation information
- Outside business hours of the responsible RA, the Swisscom hotline can be contacted at 0800 724 724, which then initializes the invalidation. The subscriber is called back to verify his identity.

[1] https://www.seco.admin.ch/sanktionen-al-qaida-taliban

[2] https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

4 Certificate life-cycle operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

Rules are set out in section 4.1.1 of the respective CP.

4.1.2 Registration process

The registration process is described in the associated CP, section 4.1.2.

4.1.3 SSCD Distribution Process

The Registration Authority registers and checks the data of the applicant. Afterwards the RA archives the data in the central systems of Swisscom, generates the personal key pair of the applicant on the pre-initialized SSCD and protects the SSCD with a PIN. Subsequently the SSCD and the PIN letter are sent to the subscriber separately.

Once the card has been received the cardholder should set a new PIN code straight away.

4.2 Certificate application processing

Rules are set out in section 4.2 of in the respective CP.

4.3 Certificate issuance

“Diamond” and “Sapphire” class certificates are only issued on Swisscom compliant SSCDs. The initialisation of the card and the generation of the key pair on the card is performed in a secure environment of Swisscom or one of its partners.

For qualified certificates, only SSCDs which have been certified in accordance with TAV [3] 3.3.3 are used.

For advanced “Sapphire” class certificates, SSCDs certified to at least FIPS 140-2 Level 3 are used.

For more details, please refer to the respective CP, chapter 4.3.

4.4 Certificate acceptance

The certificate holder is obliged to verify the correctness of the entries on his own certificate (for example, DN) and the certificate chain upon receipt. To do so the certificate display option of the Internet browser or a PDF Reader can be used.

4.4.1 Acceptance of the certificate

A certificate is deemed as accepted by the subscriber and thus valid if

- the certificate is used or
- the subscriber expressly declares his acceptance or
- no objection is submitted within 10 days of receipt.

The issuing RA must immediately revoke erroneously issued certificates.

4.4.2 Publication of the certificate

Certificates issued by Swisscom are published by the repository service immediately after being issued, provided the certificate owner gives his consent and the certificate is at all suitable for publication (which is not the case with certificates with a period of validity that is shorter than the update interval of the CRL (as with AIS OnDemand).

4.4.3 Notification to other entities

There is no provision for notifying other entities.

4.5 Key pair and certificate usage

Rules are set out in section 4.5 of in the respective CP.

4.6 Certificate renewal

Rules are set out in section 4.6 of in the respective CP.

4.7 Certificate renewal (re-key)

Rules are set out in section 4.7 of in the respective CP.

4.8 Certificate modification

A modification of certificates is not offered.

If an attribute listed in the certificate needs to be changed, a new certificate is issued.

4.9 Certificate revocation and suspension

Identification and authentication of the requestor is done as described in chapter 3.4.

The process runs as follows:

- The certificate holder or the legal person, who represents the certificate holder according to the attribute listed in the certificate, forwards the request for revocation to the appropriate registration authority.
- The registration authority verifies the identity of the applicant and the reasons for revocation.
- After a successful check, the appropriate certificate is revoked by the registration authority.
- Swisscom publishes the updated CRL with the revoked certificates.

Further details can be found in the respective CPs, chapter 4.9.

4.10 Certificate status service

Swisscom offers several procedures for checking the status of certificates.

4.10.1 Operational characteristics

A relying party can check the validity of a certificate using the following procedures

- The status of a certificate can be queried online at the Swisscom Digital Certificate Services website (http://www.swissdigicert.ch/cert_query) by selecting the menu "Certificate Inquiry". To query the status of a certificate enter a part of the CN (surname, first name, organization etc.) or the serial number of the certificate.

  This status request is not available for certificates whose period of validity is shorter than the update interval of the CRL (see section 2.3).
- An OCSP service is provided over the Internet for performing status queries.
- The status of a certificate can be queried via an LDAP query using the appropriate parameters for identifying the DN.
- An up-to-date CRL can be downloaded from the Swisscom Digital Certificate Services website (http://www.swissdigicert.ch/download_crl) in the corresponding directory.
- A web browser can be used to display the content of a certificate in detail.

4.10.2 Service availability

The online status query via the Web Server and LDAP, the CRL and OCSP are available around the clock. Swisscom provides a 99.9% availability guarantee for these services.

4.10.3 Optional features

Service availability is permanently monitored by Swisscom. All important components necessary for providing the online status query via the Web Server, LDAP and OCSP are set up redundantly and support automatic failover in the case of problems.

4.11 Termination of contract by the subscriber

Rules are set out in section 4.11 of in the respective CP.

4.12 Key escrow and recovery

In accordance with ZertES, key escrow and key recovery is not permitted for qualified signature keys and is not supported. The same applies for "Sapphire" class certificates based on the regulatory requirements of OelDI and for "Quartz" class certificates based on the requirements of the CA/Browser Forum.

5 Facility, management and personnel security controls

Infrastructural, organisational and personnel security controls for operating Swisscom Digital Certificate Services conform to the provisions of ZertES [1], TAV [3] and the referenced documents, in particular ETSI TS 101 456 [5].

Some policies like the Role Concept or the Access Policy may be dealt within separate documents, which may or may not be published.

5.1 Infrastructural security controls

5.1.1 Site location and construction

The technical systems of Swisscom Digital Certificate Services, including CA Services, are located in special secure rooms at Swisscom (so called TrustCenter). Important components are set up redundantly and are located in two separate computing centres. The buildings housing the two computing centres are far enough apart to prevent them from both being affected by natural disasters or catastrophes (more than 30 km). The buildings are in Bern and Zurich.

The rooms provide sufficient protection in terms of infrastructural security and comply with the provisions of the TAV [3] and the other referenced documents, in particular ETSI TS 101 456 [7].

5.1.2 Access controls

The operating rooms of Swisscom are secured by appropriate technical and infrastructural measures so that access is only granted to employees that have been authorised to perform a particular role within the company organisation. Access by external personnel is governed by a visitor rule. Access to the TrustCenter is protected by an access system which uses a biometric recognition procedure.

5.1.3 Power and air conditioning

The data centre is equipped with an uninterruptible power supply. Short interruptions are bridged with batteries. In the event of longer power outages the required power is supplied by diesel emergency power generators. The emergency power supply is set up redundantly (duplicate units).

5.1.4 Water exposure

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

5.1.5 Fire

The computer rooms are equipped with fire alarm systems and have smoke detectors fitted in the ceilings and floors.

Currently applicable fire prevention provisions are complied with and hand-held extinguishers are available in sufficient quantity.

5.1.6 Media storage

Media storage devices are kept in locked rooms or cabinets. Media storage devices containing sensitive data are kept in a safe if they are not located in a Swisscom data center.

5.1.7 Waste disposal

Information on electronic data carriers is properly destroyed and then disposed of by a service provider. Paper data carriers are destroyed with available paper shredders and properly disposed of by a service provider.

5.1.8 Off-site backup

The critical components for safeguarding interruption-free operation are split between two computing centers. The backups of computing center 1 are stored in computing center 2 and vice versa.

The backup of the Root Key is stored with adequate protection in a safe deposit box.

5.2 Organisational security measures

5.2.1 Trusted roles

Trusted roles have to be covered by persons that are subject to regular review. Such people are Swisscom employees, contractors and consultants who have access to the systems of Swisscom Digital Certificate Services, performing identity checks, or cryptographic operations.

The duties and obligations of persons in trusted roles are distributed so that a person cannot act alone, bypassing the security measures and may undermine the credibility of the PKI or TSA operations. The assignments of trusted roles to people is reviewed annually.

Persons who seek a trusted role shall meet the requirements of section 5.3.

5.2.2 Employees involved in the various procedures

The operation of Swisscom Digital Certificate Services requires that at least two persons acting in a trusted role work together to perform operations on the cryptographic devices in the four-eyes principle (such as activate private key, generate the CA key pair, backup of the private key etc.).

5.2.3 Identification and authentication of roles

The identification and authentication of roles is based on the role model of Swisscom Digital Certificate Services [16]. Technical access to the individual IT systems is implemented using high-level authentication (SSCD) or user names and passwords.

Cryptographic devices such as HSM and CA servers are subject to special authentication procedures. The password for "Admin" access to these components is split between the Security Device Administrator and the ISO. All access is based on the "4-eyes-principle".

5.2.4 Separation of duties

An employee can have more than one role within the same group. The assignment of roles across different groups is fundamentally prohibited because of the necessity to keep functions separate. It is also possible for role functions to be divided amongst several employees.

The following table shows which roles are absolutely incompatible (marked red).

Incompatible with	Administration/Lead	Service Manager	Product Manager	Lead Engineer	Configuration and Ops	Head of Operations	Security Device Administrator	System Administrator	1st Level Support	2nd Level Support	3rd Level Support	Security Manager on Duty	Change Manager	Building Sec. Organization	Perimeter Administrator	Perimeter Security Engineer	Local Security Officer	Controlling	Security Board	Governance Board	Change Advisory Board	Information Sec. Officer	Internal Audit	System Auditor	Miscellaneous	Legal & Compliance	Human Resources
Administration/Lead																											
Service Manager																							🟥	🟥			
Product Manager																							🟥	🟥			
Lead Engineer						🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥				🟥	🟥	🟥	🟥			
Configuration and Ops																											
Head of Operations				🟥			🟥															🟥	🟥	🟥			
Security Device Administrator				🟥		🟥																🟥	🟥	🟥			
System Administrator				🟥																		🟥	🟥	🟥			
1st Level Support				🟥																		🟥	🟥	🟥			
2nd Level Support				🟥																		🟥	🟥	🟥			
3rd Level Support				🟥																		🟥	🟥	🟥			
Security Manager on Duty				🟥																		🟥	🟥	🟥			
Change Manager				🟥																		🟥	🟥	🟥			
Building Sec. Organization				🟥																		🟥	🟥	🟥			
Perimeter Administrator				🟥																		🟥	🟥	🟥			
Perimeter Security Engineer				🟥																		🟥	🟥	🟥			
Local Security Officer				🟥																		🟥	🟥	🟥			
Controlling																											
Security Board																											
Governance Board																											
Change Advisory Board				🟥																		🟥	🟥	🟥			
Information Sec. Officer				🟥		🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥				🟥		🟥				
Internal Audit		🟥	🟥	🟥		🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥				🟥	🟥					
System Auditor		🟥	🟥	🟥		🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥				🟥						
Miscellaneous																											
Legal & Compliance																											
Human Resources																											

5.3 Personnel security controls

5.3.1 Requirements of all employees

Swisscom employees responsible for operating the CA or carrying out maintenance must fulfil all the necessary requirements with regard to trustworthiness, integrity, reliability and requisite skills. In addition to a general education in the area of IT, the employees also need to have the requisite skills for performing their particular roles in the following areas:

- Security technology, cryptology, electronic signatures, PKI,
- international standards, technical standards,
- operating systems, TCP/IP networks and LDAP.

5.3.2 Background checks for employees

Records from criminal and debt collection register are kept for all employees of Swisscom Digital Certificate Services, Platform Management & Operations. These need to be re-submitted every three years.

Non-employees are only allowed to enter operating rooms in the accompaniment of authorised employees of Swisscom.

5.3.3 Training requirements

Only qualified employees are deployed in the business organisation of Swisscom Digital Certificate Services. In addition, regular training sessions are held by competent personnel for all business organisation employees.

Employees are only assigned a specific role once they have demonstrated that they have the requisite skills.

5.3.4 Training frequency

Training frequency is geared towards requirements. Training sessions are held in particular when new guidelines, IT systems and security techniques are introduced.

5.3.5 Job rotation frequency and sequence

Job rotation is based on the requirements of Swisscom Digital Certificate Services or a particular employee. A change in workplace is not always necessary.

5.3.6 Sanctions for unauthorised actions

Unauthorised actions that compromise the security of the IT systems of Swisscom Digital Certificate Services or violate data protection provisions are subject to disciplinary action. If this involves criminal proceedings, the relevant authorities will be informed.

5.3.7 Contract of employment requirements

Employment contracts of Swisscom Digital Certificate Services employees are subject to Swiss law.

All employees need to sign a non-disclosure agreement as a supplement to their contract of employment.

5.3.8 Documentation supplied to personnel

The following documents are available to employees of Swisscom Digital Certificate Services:

- Certificate Policies (CP)
- Certificate Practice Statement (CPS)
- Security Concept
- Description of roles
- Process descriptions and formulae for regular operations
- Documented procedures for emergency situations
- Documentation of IT systems
- User guides for the deployed software

5.4 Security monitoring

5.4.1 Monitored events

The following measures have been implemented in order to repel attacks and ensure that the Swisscom Digital Certificate Services infrastructure is functioning correctly. The following classes of events are recorded in the form of log files or paper protocols:

- Operation of IT components, including
  - Hardware booting procedures
  - Failed login attempts
  - Issuing and cancellation of permissions
  - Installation and configuration of software
- All transactions of the certificate authority, including
  - Certificate requests
  - Certificate deliveries
  - Certificate publications
  - Certificate revocations
  - Key creations
  - Certificate creations
- Amendments to guidelines and the operations manual, including
  - Role definitions
  - Process descriptions
  - Changes in responsibilities
- Physical Security
  - Access to data center
  - Technical alarms
  - Break-in reports

5.4.2 Frequency of processing log

The audit log is examined in accordance with internal guidelines.

5.4.3 Retention period for audit log

Security-relevant audit logs are stored in accordance with legal provisions. The retention period for audit logs of key and certificate management corresponds to the period of validity of the certificate of the CA plus 11 years.

5.4.4 Protection of audit logs

Electronic log files are transferred to an external Syslog server where they are protected from access, deletion and manipulation and only accessible to system and network administrators.

5.4.5 Audit log backup

Audit logs are backed up regularly together with other relevant data of the Swisscom Digital Certificate Services infrastructure.

5.4.6 Monitoring systems

Availability of all important service components are monitored proactively 7x24. The CA and the repository service are monitored using an appropriate procedure and protected against unauthorised modifications.

5.4.7 Notification in the event of serious incidents

The Information Security Officer (ISO) of the platform, followed by the Security Board, must be informed immediately about serious incidents. An action plan is devised in collaboration with system administrators to adequately respond to the incidents. If necessary, the executive board may be informed.

5.4.8 Vulnerability assessment

A vulnerability assessment is performed using automated tools in the perimeter (DMZ) and network segment of the CA. The results are checked by the ISO.

5.5 Archiving

5.5.1 Archived data

Data related to the certification process is archived:

- All certificates issued by the certification authority
- Revocation requests
- Certificate revocation lists (CRL)

Other internally required information that needs to be archived includes the following:

- CA root certificate and CA certificates for “Diamond”, “Sapphire”, “Emerald”, “Ruby”, “Quartz” and “Time-Stamping”, including the associated private keys
- Contracts and certificate applications containing personal information about the subscriber
- Activity journal of Swisscom Digital Certificate Services

Devices and applications for reading and representing the archived data are kept as long as it is necessary to meet regulatory requirements. Alternatively a data conversion must be performed.

5.5.2 Retention period of archived data

The rules described in section 5.4.3 apply.

5.5.3 Protection of archive

Appropriate measures are adopted to ensure that data cannot be modified or deleted. It also needs to be ensured that any personal data contained in the archive cannot be read or copied by unauthorised persons.

5.5.4 Data security concept

The data listed in sections 5.4.1 and 5.5.1 is regularly backed up offline in accordance with a data security concept. Key features of the data security concept:

- incremental backup each working day
- weekly complete backup
- monthly archive backup

Backups are always stored in duplicate in the two different data centers.

5.5.5 Time stamping requirements

The requirements in VZertES [2], section 12 and TAV [3], section 3.5 apply.

5.5.6 Archiving system

An internal archiving system is used.

5.5.7 Procedures for obtaining and verifying archived data

The ISO can authorise the querying and checking of archived data.

5.6 Key changeover

The period of validity of keys is set out in section 6.3.2. The rules for key changeovers for subscribers are set out in the respective CP. If one of the certification authority's keys is compromised, the rules in section 5.7.3 apply.

5.7 Compromise and recovery

5.7.1 Procedures for handling security incidents and compromise

The procedures for handling security incidents and the compromise of private keys belonging to the certification authority are documented in set of emergency procedures, which are available to all employees.

Security incidents can be reported to the relevant RA partner or directly to the Swisscom Call Center at 0800 724 724.

5.7.2 Procedures for IT systems

If defective or manipulated computers, software and/or data are discovered within the CA, which impacts the processes of the certification authority, the operation of the respective IT system must be suspended immediately. The IT system is set up on replacement hardware using recovered software and backup data. After being checked it is put into operation securely. The faulty or modified IT system is then analysed. If there is a suspicion of deliberate intervention, legal steps may be taken. Security arrangements will also be evaluated and revised to take account of any vulnerabilities. Additional preventative measures may also be adopted to prevent similar incidents occurring. Employees of the certification authority work in collaboration with the experts of the Swisscom CERTs in such cases. If incorrect information is contained in a certificate, the subscriber is informed immediately and the certificate revoked.

5.7.3 Compromise of private keys of a CA

If the private key of an issuing CA has been compromised, or there is justified suspicion of a compromise, the Security Board must be informed immediately. The Security Board will investigate the actual or suspected compromise and, if necessary, will order the revocation of the certificate in question. This involves taking the following measures:

- Immediate information to all directly affected subscribers;
- Revocation of the CA certificate and all certificates that were certified with the certificate. Possible deactivation of the repository service and status requests to prevent incorrect or invalid statements being issued by the service;
- Generation of a new key pair and a certificate for the CA;
- Publication of the CAs certificate;
- Issuing of new certificates for subscribers in accordance with Security Board guidelines.

5.7.4 Business continuity following a disaster

A resumption of certification operations following a disaster situation is part of emergency planning and can take place within a short period of time provided the security of the certification service can be guaranteed. The evaluation of the security situation is the responsibility of the Security Board.

5.8 Termination of operations

If certification operations are to be terminated, the following measures as required per law must be taken:

- Inform the certification authority and SAS/SECO;
- Inform all subscribers, registration authorities and affected organisations at least three months before termination of operations;
- Inform the public;
- Revoke all certificates that are still valid by the termination deadline;
- Transfer the final Certificate Revocation List (CRL), the transcription journal and all supporting documents to the authority designated by SAS;
- Destroy the private keys of the certification authority securely.

6 Technical security controls

The technical security requirements of Swisscom or a RA are determined by the services offered. The actual security level in terms of basic availability, integrity, confidentiality and authenticity are set out in a security concept. The security concept is not published but is made available as part of the conformity check.

If individual security measures are not specified in this CPS, they can usually be taken from the respective catalogue of measures of the ISO/IEC 27001.

6.1 Key pair generation and installation

6.1.1 Key pair generation

The key pairs of the root CA are generated on a dedicated HSM. The IT system containing the root CA is not connected to any network. Keys are exclusively stored on an HSM and protected by multiple PED keys. A backup of the HSM is stored securely.

The key pairs of the level 1 CA are generated and stored on a separate HSM. They are protected by multiple PED Keys. A HSM backup is kept safely.

Key pairs for “Diamond” and “Sapphire” class signature and authentication certificates are only generated and stored inside the SSCD which are compliant with the Swiss Signatures Act (ZertES) and are conform at least to FIPS 140-2 Level 3.

6.1.2 Private Key delivery to subscriber

Key pairs for signing and authentication certificates of the classes "Diamond" and "Sapphire" are produced exclusively on a SSCD. Does the subscriber hold the key pair on a SSCD, it is passed to him in a secure manner.

Certificates of the certificate classes "Ruby" and "Emerald" are produced by the RA. At the request of the customer, encryption certificates can be created in such a way as to enable the key pair to be restored in the event of the SSCD being lost.

If the key pair is generated by the RA, soft certificates are delivered to the subscriber in encrypted containers (PKCS#12). The PIN for unlocking the container is delivered separately.

6.1.3 Public key delivery to certificate issuer

The RAs which issue “Diamond” and “Sapphire” class certificates on SSCDs may only submit certificate requests via the front-end of the Card Management System provided by Swisscom Digital Certificate Services. The Card Management System ensures that the signed public key is sent to the CA in a PKCS#10 request via secure connection.

6.1.4 Public CA key delivery

All participants of Swisscom Digital Certificate Services can retrieve the public signature verification key of the Swisscom Digital Certificate Services root CA and the subordinate CAs in PKCS#7 or binary format (DER) via the repository service (cf. 2.1).

6.1.5 Key sizes

The cryptographic algorithms used and their key lengths are based on ETSI TS 102 176 referred to in TAV and are currently:

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 CAs of the next level (Level 1)
- RSA 2048 SHA-256 for the certificates and timestamping with the identifiers CA 2 and CA 3

Root EV CA 2 (OID 2.16.756.1.83.21)

- RSA 4096 SHA-256 for the CA 2 Root-Key
- RSA 2048 SHA-256 for the CA of the next level (Level 1)
- RSA 2048 SHA-256 for certificates of class Quartz

6.1.6 Public key parameters and quality checking

Parameters are based on TAV [3] guidelines and are created by the CA. The parameters are selected carefully during creation.

6.1.7 Key usage purposes and limitations

Key usage purposes and limitations are entered in the corresponding X.509 v3 field (keyUsage) (please see addendum to the CPS [9], section 2) and are contained in the respective CP.

6.2 Private Key protection

The private key of the root CA, the CAs of the next level (Level 1) and timestamps are generated and stored in the HSMs. Signatures are processed in the HSM and the corresponding private key never leaves the HSM.

“Diamond” and “Sapphire” class private keys are generated and stored in a SSCD. Signatures are processed on the SSCD. The SSCD used meets the requirements of TAV section 3.3.3.

A special environment is created on the SSCD for the qualified signature key. This ensures that the private key is adequately protected and under the sole control of the subscriber.

6.2.1 Cryptographic module standards

The HSM modules and SSCD used for certification meet the requirements of TAV [3]:

HSM: SafeNet Luna SA

- FIPS 140-2 Level 3

6.2.2 Private key sharing

There is no provision for sharing the private keys of Swisscom Digital Certificate Services Root CA and the CA Services.

6.2.3 Private key escrow

The private keys of subscribers are not escrowed in the case of qualified signature keys. The same applies for signature keys of the Sapphire certificate class.

A key escrow can be offered for all other classes at the request of the subscriber.

6.2.4 Private key backup

It is not possible to back up Diamond and Sapphire class private keys if a Smart Card is used.

If an HSM is used, it is possible to export the signature key and make a backup in the appropriate way, as long as the exported signature key has the same level of protection as when it is inside the HSM and there is no possibility of the signature key being used outside the HSM.

Copies of the key pairs of the Root CA and of the Issuing CAs are made and stored on an HSM in a safe. The private keys are protected by PED Keys.

6.2.5 Private key archiving

The private signatures and authentication keys of “Diamond” and “Sapphire” class subscribers are not archived.

6.2.6 Creation and Storage of Private keys

“Diamond” and “Sapphire” class signature and authentication keys as well as the CA keys are only created and stored in cryptographic modules (HSM and Smart Cards).

6.2.7 Method of activating private keys

6.2.7.1 The subscriber keeps certificate and private key on its own SSCD

“Diamond” and “Sapphire” class private keys are activated by entering activation data (e.g. PIN) by the subscriber.

6.2.7.2 The subscriber keeps certificate and private key in the All-in Signing Service

The transfer of the activation data is not applicable. The declaration of intention to use the private key is done via appropriate means (e.g. Mobile ID [18]).

6.2.7.3 Private keys of the CAs

The black PED key is used for activating the private keys of the issuing CAs. This PED key is held by the role “Secure Device Administrator (SECADM)”. Activation can only take place in the presence of a second person which holds another PED key (four-eyes-principle).

6.2.8 Method of deactivating private keys

Deactivation of a private key is done by removing the activation data (e.g. PIN) under authority of the subscriber.

6.2.9 Method of destroying private keys

The four-eyes principle is applied when destroying private keys of the Root CA and the related issuing CAs it operates. Destroying the keys is the responsibility of the ISO and SDADM roles.

6.2.10 Cryptographic module rating

Cf. chapter 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys are archived both by the repository service and on storage media for backup purposes.

6.3.2 Validity of certificates and key pairs

Certificates issued by the Root CA and CA Services have the following periods of validity:

- Certificate of the Root CA, up to 20 years
- Certificates of the subsequent issuing CAs, up to 10 years
- “Diamond”, “Sapphire” and “Emerald” class certificates, up to 3 years
- “Quartz” class certificates up to 2 years

- "Ruby" class certificates, up to 5 years

The permitted usage period for key pairs is basically equivalent to the period of validity of the related certificates. The use of available key pairs for re-certification purposes is only permitted for encryption certificates if the recommended algorithms and key lengths allow this (cf. chapter 6.1.5 and the related CP, chapter 4.7.1).

6.4 Activation data

Trivial combinations cannot be chosen for PINs used for activating private keys. The PIN should contain both alphanumeric characters and special symbols and be at least 6 characters long.

6.4.1 Activation data protection

a. *The subscriber keeps certificate and private key on its own SSCD:*

   Activation data must be kept secret. For "Diamond" class certificates the key is blocked after 4 failed attempts.

   In the case of "Sapphire" class certificates it must be possible to detect incorrect and consecutive activation attempts and block signature key usage after a predetermined number of attempts.

b. *The subscriber keeps certificate and private key in the All-in Signing Service:*

   The transfer of the activation data is not applicable. The declaration of the intention to use the private key is done via appropriate means (e.g. Mobile ID [13]).

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

All applications within the CA are run exclusively on hardened operating systems (operating systems optimised for security). Change auditing software is also used for the CA and Directory Service. This software places a hash value on the configuration files in order to detect modifications.

The following security measures are also implemented:

- Restrictive access controls
- User authentication and authorisation on a "need-to-know" and "need-to-do principle"
- Traceability through log files and a common, reliable time basis for all CA systems

6.5.2 Security controls rating

Security measures are periodically examined.

6.6 Lifecycle of 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

Security management covers the following aspects:

- annual audit (conformity check by internal and external auditors)
- Regular assessment and further development of the security concept (annual)
- Security check during normal operations (cf. 5.4)
- Regular integrity check of individual applications and operating systems
- Central logging of all security-related procedures
- Cooperation with Swisscom CERT
- Installation of upgrades and patches as required
- Use of productive systems only after test systems have been released

6.7 Network security controls

The CA network is divided into different security zones which are isolated from one another by a firewall. Intrusion prevention and/or detection systems are also used to prevent attacks over the Internet and the Intranet. Critical security incidents are investigated and processed immediately in collaboration with Swisscom CERT.

6.8 Time stamping

Swisscom Digital Certificate Services provides a time stamping service in accordance with the requirements described in TAV [3], section 3.5. The time base is achieved with an appliance from Meinberg, which is synchronised via a GPS external antenna and verified via a DCF-77 signal. The time base is distributed via NTP to all servers of the Swisscom Digital Certificate Service infrastructure.

The time stamp service is operated on the CA's HSM, thus it is provided by a SafeNet Luna SA device. Please consult the CP of the time stamping service for more details.

7 Certificate, CRL and OCSP profiles

Profiles for certificates, revocation lists and online status requests are defined in accordance with the guidelines of the TAV [3] and the other referenced documents, in particular ETSI 101 456 [5] and set out in detail in the addendum to this CPS [14].

For further details on the certificate profiles and extensions please refer to the respective CP, chapter 7.

8 Compliance Audit and other assessments

Rules are set out in the respective CP.

9 General provisions

9.1 Fees

Fees for services provided by Swisscom Digital Certificate Services are detailed in the pricelist, which can be requested from the contact address in section 1.5. The pricelist of the RA-contractors (E-RAs/TPS) are available on request from the corresponding E-RA/TPS. Additional services that are not covered by the pricelist can be billed separately.

9.2 Financial responsibility

9.2.1 Insurance coverage

Insurance coverage provided by Swisscom covers the legal liability as per ZertES section 16 und the requirements of the CA Browserforum. For the mentioned damages and costs, a common sub-limit of CHF 2 million per event and CHF 8 million per policy year applies.

Otherwise the Terms and Conditions of "Enterprise Customers" of Swisscom (Switzerland) Ltd apply.

9.2.2 Insurance coverage for subscribers and RAs

The subscribers and RA partners are responsible for taking out adequate insurance coverage for their liability obligations relating to signature legislation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

All information regarding participants and applicants that does not fall under chapter 9.3.2 is classed as confidential information. Such information includes business plans, sales information, information about business partners and all information communicated during the registration process.

9.3.2 Information not within the scope of confidential information

All information contained in the issued certificates and the certificate revocation list, whether explicitly (e.g. DN elements, e-mail address) or implicitly (e.g. information regarding certification), or which can be derived therefrom is not classed as confidential.

9.3.3 Responsibility to protect confidential information

Swisscom is responsible for adopting measures to protect confidential information. Information may only be processed as part of the service provision and only disclosed to third parties if a confidentiality agreement has been signed beforehand and the employees involved have undertaken to comply with the legal provisions pertaining to data protection.

RA contracting partners who submit and receive information to and from Swisscom as part of the certificate application process are not considered to be third parties. Documents can be viewed for auditing purposes in the presence of the Swisscom Digital Certificate Services security officer or an appointed representative.

9.4 Protection of personal information

Swisscom only gathers, stores and processes information that is necessary for providing services, for developing and maintaining customer relations (i.e. to guarantee a high-quality service), for ensuring the security of operations and infrastructure and for billing purposes.

To prevent misuse of data by Spam senders, email addresses (if included in the certificate) can only be retrieved by authorized users. Email addresses will not be provided to non-registered users. In the LDAP directory, no systematic wildcard queries are supported.

9.4.1 Responsibility to protect personal information

Swisscom and the registration authorities operating on its behalf are obliged to handle personal information in compliance with the following principles:

- Personal data may only be obtained in accordance with the law
- Personal data must be processed in good faith and to a reasonable extent.
- Private information may only be processed for the purpose stated when obtaining it and in compliance with legal provisions (section 4 DSG).
- Personal information must not be used for commercial purposes (section 14, para. 1 ZertES).

9.4.2 Disclosure pursuant to judicial or administrative process

Swisscom is subject to Swiss law and is obliged to disclose customer information to government authorities in accordance with applicable law if requested to do so.

9.4.3 Other information disclosure circumstances

Information is not disclosed to third parties in any other circumstances.

9.5 Intellectual property rights

Swisscom is the owner of the intellectual property rights of the following documents:

- The present CPS
- The associated CPs
- The associated Terms of Use

Swisscom authorises the RA partners and subscribers to forward the documents listed above unaltered to third parties. Additional rights are not granted. In particular, the forwarding of modified versions and insertion in other documents or publications without written consent from Swisscom is prohibited.

9.6 Representations and warranties

9.6.1 Commitment of Swisscom

Swisscom undertakes in its role as CSP to perform all the tasks described in this CPS and the associated CPs in accordance with the provisions of the ZertES and all other implementation provisions (TAV [3]).

9.6.2 Commitment of RA contractors and Registration Authorities

The RA contracting partners are contractually obliged to comply with all requirements pursuant to the ZertES [1] and the TAV [3], chapter *3.4.1 Registration, administration and revocation of certificates for third parties*.

All RA contracting partners operating on behalf of Swisscom are obliged by Swisscom to perform all the tasks and duties described in this CPS and the associated CPs. Compliance with the relevant CP/CPS must be declared in writing by the RA operators with respect to Swisscom. Likewise, the roles and responsibilities of the RA must be documented and communicated by Swisscom.

With a RA, that issues certificates of the class "Diamond", compliance with the requirements of Swisscom and the Swiss Signatures Act is reviewed regularly.

9.6.3 Commitment of Subscribers

In organization certificates, the organization in whose name the certificate is issued (see O-field), is responsible for the adoption of internal organizational directives that rule the use and access to the certificate and its blocking (e.g. storage of the smart card, the password, the lock password, etc. .).

The rules under section 4.5.1 apply.

9.6.4 Commitment of Relying parties

The rules under section 4.5.2 apply.

9.6.5 Commitment of other participants

If other participants are involved as service providers in the certification process, Swisscom is responsible to ensure that the service providers comply with the CP and CPS.

9.7 Liability of Swisscom

Swisscom is liable to the holder of the signature key and any third parties who rely on a valid certificate for damages they sustain on account of Swisscom's' failure to meet its obligations regarding the ZertES [1] and the TAV [3].

Swisscom is not liable for damages arising from the non-compliance with or transgression of a usage restriction contained in the certificate.

In all other instances Swisscom shall be liable as follows:

- In the event of any breach of contract, Swisscom shall be liable for any proven damage, unless Swisscom is able to prove that the damage was sustained through no fault of its own.
- Swisscom shall have unlimited liability for damages arising from intentional conduct or gross negligence.
- In the event of simple negligence, Swisscom shall be liable for personal injury up to an unlimited amount; for material damage up to CHF 5000 per event and calendar year[3].
- In the event of simple negligence, Swisscom shall be liable for financial loss up to the equivalent value of the agreed services provided during the current year of contract, up to a maximum of CHF 5000 per event and calendar year [3].

[3] For qualified certificates of classes "Diamond", "Diamond SuisseID" and "Quartz" higher amounts apply, see the associated CP, Section 9.7

- Swisscom shall under no circumstances be held liable for consequential loss or loss of profits or data.
- Swisscom shall not be liable for damages and the consequences of delays caused by force majeure, natural disasters (e.g. lightning, weather-related events), power outages, war, strikes, unforeseen restrictions imposed by authorities, the use of call baring, PC diallers, hacker attacks, virus attacks on data processing equipment (e.g. Trojan horses), etc.

If Swisscom is unable to fulfil its contractual obligations, the performance of contract or the deadline for performance of contract will be postponed commensurate with the delay caused by the event that occurred. Swisscom shall not be liable for any damages sustained by the customer as a consequence of the contract performance being postponed.

9.8 Liability of the Subscriber

The subscriber (or the organisation mentioned in the O-field of the certificate) shall be liable in accordance with the contractual agreement with the RA for damages suffered by them because he did not comply with his contractual obligations (in particular the arrangements for the use of the certificate).The subscriber (or the organisation mentioned in the O-field of the certificate) has exclusive liability for using the secret key on which the certificate is based.

9.9 Effective Date and termination

9.9.1 Effective Date

This CPS and the associated CPs enter into force on the day they are published by the information service (cf. chapter 2.2) of Swisscom Digital Certificate Services.

9.9.2 Termination

This document remains in effect until

- it is replaced by a newer version or
- the operations of the CA of Swisscom Digital Certificate Services are terminated.

9.9.3 Effects of termination

In the event of this CPS and the associated CPs being terminated, the subscribers are bound to the related Terms of Use for the remainder of the term of validity of already issued certificates.

9.10 Individual notices and communication with participants

Swisscom communicates with the subscriber via signed email, if the email address is known, or letter.

Correspondence with participants takes place by means of signed forms via e-mail or letter. Announcements and news are published on the Swisscom (Switzerland) Ltd. homepage.

9.11 Policy amendments

Minor changes with no or only minimum effect for users are entered into force directly by Swisscom. Major changes are implemented by arrangement with and approval of the certification authority. Changes are entered into a journal.

If the amendments involve security related aspects or affect the processes of the parties listed in section 1.3, the latter must be informed without delay.

A formal approval of the CPS and CPs is done by the Governance Board.

9.12 Dispute resolution provisions

In case of conflict, the parties referred to in Section 1.3 try to find an amicable settlement of disputes.

9.13 Applicable law and place of jurisdiction

All legal relations in connection with the services of Swisscom according to this document are subject to Swiss law, excluding the *Conflicts of Law* rules of the private international law and the United Nations Convention on the International Sale of Goods of April 11th 1980.

The sole place of jurisdiction is Bern.

9.14 Compliance with applicable law

Swisscom reserves the right to operate as a CSP in terms of the Swiss Signatures Act ZertES [1] and to issue qualified and advanced certificates.

9.15 Other provisions

9.15.1 Scope and applicability

All provisions contained in this CPS and the associated CPs apply between Swisscom and the RAs. The RAs in turn agree to integrate these rules in accordance with the agreements between them and the subscribers. If Swisscom directly concludes agreements with the subscribers, the present CPS and the CP of the related certificate class are integrated into it.

9.15.2 Language

In order to facilitate international cooperation with other certification authorities, a translation of the CPS is published. In case of doubt, the German version of the text is legally binding.

9.15.3 Validity

The release of a new version replaces all previous versions.

9.15.4 Assignment of rights and obligations

The subscriber is not permitted to transfer his rights and obligations. Swisscom is entitled to transfer its rights and obligations to third parties, in particular to other Swisscom business units.