Swisscom
Digital Certificate Services

Certification Practice Statement （CPS）

For the:

- Swissocm Root CA 1 (OID: 2.16.756.1.83.0.1:2.16.756.1.83.0.1) und Swisscom Root CA 2 (OID: .16.756.1.83.2.1:2.16.756.1.83.2.1)
- Level 1 CAs （Diamond, Sapphire, Ruby, Emerald, Time Stamp, Customer）
- User certificates （Diamond, Sapphire, Ruby, Emerald, E-RA）
- Time Stamp Services

Abstract	Certification Practice Statement for qualified and advanced certificates of Swisscom Digital Certificate Services, a Swisscom service for issuing digital certificates for the creation of qualified electronic signatures in accordance with the Swiss Federal Act on Electronic Signatures （ZertES）
Name	002_cps_swisscom_digital_certificate_services_2 16 756 83 2 1_v2_0_en.doc
Version	2.0
Classification	Unclassified
Project Name	“Hermes”
OID	2.16.756.1.83.0.1 (Swisscom Root CA 1) 2.16.756.1.83.2.1 (Swisscom Root CA 2)
CA Names	Swisscom Root CA 1, Diamant CA 1, Saphir CA 1, Rubin CA 1, Swisscom Root CA 2, Diamant CA 2, Saphir CA 2, Rubin CA 2,

	Smaragd CA 1, Timestamp CA 1, Diamant SuisseID CA 1 Saphir SuisseID CA 1 Test CA 1	Smaragd CA 2, Timestamp CA 2, Diamant SuisseID CA 2 Saphir SuisseID CA 2
CA Owner	Swisscom （Schweiz） AG	
Language Version:	English （original version in German is legally binding）	
CP Compliance start:	17. Oktober 2005 (Swisscom Root CA 1) 1. Januar 2011 (Swisscom Root CA 2)	
Document approval	Swisscom （Schweiz） AG, Head of ICT Security Services	
Signature		

Document history

Version	Date	Responsible	Comments/type of revision
1.0	2 December	Project Team	Changes to KPMG Audit
1.1	8 May 2006	Project Team	Amendments to Sapphire and Emerald and various other modifications
1.2	25. Feb. 2008	Daniel Keller	Various Modifications
1.3	8. Jul 2010	Project Team	Updated Service Structure
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
2.2	16.10.2012	Governance Board	Freigabe durch committee

Reference documents:

Reference	Description
[1]	ZertES: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Federal Act on Electronic Signatures, ZertES) of 19 December 2003, hereinafter referred to as Swiss Signatures Act.
[2]	VZertES: Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (Ordinance on Certification Services in the Field of Electronic Signatures, VZertES) dated 3 December 2004
[3]	TAV: Technical and administrative provisions for certification services in the field of electronic signatures, version 2: 29.7.2005, SR 943.032.1
[4]	IETF RFC 3647 (2003): "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework"
[5]	ETSI TS 101 456 V1.3.1 (2005-05): Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates
[6]	IETF RFC 3280 (2002) "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
[7]	IETF RFC 2560 (1999) "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP"
[8]	SR 641.201.1 Ordinance of the FDF on Electronically Transmitted Data and Information (EIDI-V) dated 30 January 2002 (as of 19 February 2002)
[9]	SR 641.201.1.1 Technical and administrative guidelines for certification services in the field of electronically transmitted data and information (EIDI-V) in connection with the issuing of advanced certificates

swisscom

Contents

1 Introduction 8
1.1 Overview 10
1.2 Document Identification 10
1.3 Swisscom Digital Certificate Services participants 12
1.3.1 Certification Authorities (CAs) 12
1.3.2 Registration Authorities (RAs) 13
1.3.3 Subscribers 14
1.3.4 Relying parties 15
Information on relying parties is available in the respective CP 15
1.3.5 Other participants 15
1.4 Certificate usage 15
1.5 Policy administration 15
1.5.1 Organisation and contact address 15
1.5.2 Contact person 15
1.5.3 Persons responsible for the CPS 16
1.5.4 Approval procedure 16
1.5.5 Policy amendments 16
1.6 Terms and keywords 16

2 Publication and Repository Service 20
2.1 Repositories 20
2.2 Publication of certificate information 20
2.3 Frequency of publication 21
2.4 Access controls on repositories 21

3 Identification and authentication 21
3.1 Naming 21
3.1.1 Types of names 21
3.1.2 Need for names to be meaningful 23
3.1.3 Anonymity / pseudonymity 24
3.1.4 Rules for interpreting various name forms 24
3.1.5 Uniqueness of names 24
3.1.6 Recognition, authentication and role of trademarks 24
3.2 Initial identity validation 24
3.2.1 Method for proving possession of private key 24
3.2.2 Authentication of a legal entity 24
3.2.3 Authentication of a natural person 25
3.2.4 Non-verified information 25
3.3 Identification and authentication for re-key requests 25
3.3.1 Identification and authentication for routine re-key requests 25
3.3.2 Identification and authentication for re-key after revocation 25
3.4 Identification and authentication for revocation requests 25

4 Certificate life-cycle operational requirements 27
4.1 Certificate application 27
4.1.1 Who can submit a certificate application 27
4.1.2 Registration process 27
4.2 Certificate application processing 28
4.2.1 Performing identification and authentication functions 28
4.2.2 Approval or rejection of certificate applications 28
4.2.3 Processing time 28
4.3 Certificate issuance 28
4.4 Certificate acceptance 28
4.4.1 Acceptance of the certificate 28
4.4.2 Publication of the certificate 28
4.4.3 Notification to other entities 28
4.5 Key pair and certificate usage 29
4.6 Certificate renewal 29
4.7 Certificate renewal (re-key) 29
4.8 Certificate modification 29
4.9 Certificate revocation and suspension 30
4.10 Certificate status service 30
4.10.1 Operational characteristics 30
4.10.2 Service availability 30
4.10.3 Optional features 30
4.11 Termination of contract by the subscriber 30
4.12 Key escrow and recovery 31

5 Facility, management and personnel security controls 32
5.1 Infrastructural security controls 32
5.1.1 Site location and construction 32
5.1.2 Access controls 32
5.1.3 Power and air conditioning 32
5.1.4 Water exposure 32
5.1.5 Fire 32
5.1.6 Media storage 33
5.1.7 Waste disposal 33
5.1.8 Off-site backup 33
5.2 Organisational security measures 33
5.2.1 Trusted roles 33
5.2.2 Employees involved in the various procedures 43
5.2.3 Identification and authentication of roles 44
5.2.4 Separation of duties 44
5.3 Personnel security controls 45
5.3.1 Requirements of all employees 45
5.3.2 Background checks for employees 46
5.3.3 Training requirements 47
5.3.4 Training frequency 47

5.3.5 Job rotation frequency and sequence 47
5.3.6 Sanctions for unauthorised actions 47
5.3.7 Contract of employment requirements 47
5.3.8 Documentation supplied to personnel 47
5.4 Security monitoring 48
5.4.1 Monitored events 48
5.4.2 Frequency of processing log 48
5.4.3 Retention period for audit log 48
5.4.4 Protection of audit logs 49
5.4.5 Audit log backup 49
5.4.6 Monitoring systems 49
5.4.7 Notification in the event of serious incidents 49
5.4.8 Vulnerability assessment 49
5.5 Archiving 49
5.5.1 Archived data 49
5.5.2 Retention period of archived data 50
5.5.3 Protection of archive 50
5.5.4 Data security concept 51
5.5.5 Time stamping requirement 51
5.5.6 Archiving system 51
5.5.7 Procedures for obtaining and verifying archived data 51
5.6 Key changeover 51
5.7 Compromise and recovery 51
5.7.1 Procedures for handling security incidents and compromisation 51
5.7.2 Procedures for IT systems 51
5.7.3 Compromisation of private keys of the certification authority 53
5.7.4 Business continuity following a disaster 53
5.8 Termination of operations 53

6 Technical security controls 56
6.1 Key pair generation and installation 56
6.1.1 Key pair generation 56
6.1.2 Private key delivery to subscriber 56
6.1.3 Public key delivery to certificate issuer 56
6.1.4 Public CA key delivery 56
6.1.5 Key sizes 57
6.1.6 Public key parameters and quality checking 57
6.1.7 Key usage purposes and limitations 57
6.2 Private key protection 57
6.2.1 Cryptographic module standards 57
6.2.2 Private key sharing 58
6.2.3 Private key escrow 59
6.2.4 Private key backup 59
6.2.5 Private key archiving 59
6.2.6 Private key transfer to a cryptographic module 59
6.2.7 Private key storage on cryptographic module 59
6.2.8 Method of activating private key 59

6.2.9 Method of deactivating private key 59
6.2.10 Method of destroying private key 59
6.2.11 Cryptographic module rating 60
6.3 Other aspects of key pair management 60
6.3.1 Public key archival 60
6.3.2 Validity of certificates and key pairs 60
6.4 Activation data 60
6.4.1 Activation data generation and installation 60
6.4.2 Activation data protection 60
6.4.3 Other aspects 60
6.5 Computer security controls 61
6.5.1 Specific computer security technical requirements 61
6.5.2 Security controls rating 62
6.6 Lifecycle of security controls 62
6.6.1 Software development 62
6.6.2 Security management 62
6.7 Network security controls 62
6.8 Time stamping 62

7 Certificate, CRL and OCSP profiles 63
7.1 Certificate profiles 63
7.1.1 Root CA certificate 63
7.1.2 CA qualified certificate (Diamond) 64
7.1.3 Qualified user certificate (Diamond) 66
7.1.4 Ruby and Emerald user certificates for secure e-mail and encryption 67
7.1.5 Sapphire/Ruby user certificates for authentication purposes 70
7.2 CRL profile 73
7.3 OCSP profile 73
7.4 TSA Profile 75

8 Compliance check 78

9 General provisions 78

10 Identification and authentication 78

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, a Swisscom (Schweiz) AG service [hereinafter referred to as Swisscom (Schweiz) AG] which issues qualified and advanced certificates in accordance with the Swiss Signatures Act, ZertES [1] and the referenced technical and administrative implementation guidelines TAV[3] and VZertES [2].

Associated with this document are the respective Certificate Policies (CP) of the certificate classes "Diamond" (qualified), "Sapphire" (advanced), "Ruby" and "Emerald", in addition to Time Stamp Services.

The present CPS describes with two different CA generations. The first generation ends with CA 1 and uses SHA-1 as hashingalgorithm. The second CA generation ends with CA 2 and uses SHA-256 as hashingalgorithm. The numbering within a CA hierarchy is kept constant, this means all CA 1 issuing CAs are issued by Root CA 1 and all CA 2 issuning CAs are issued by Root CA 2. If not otherwise specified all specifications in this document refer to both CA generations.

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 available 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.

Electronic certificates are used to assign a public cryptographic key to a person so as to 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 Signatures Act (ZertES [1]), the Ordinance on Electronic Signatures (VZertES [2]) and the technical and administrative guidelines 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, Article 14, Paragraph 2^{bis} of the Swiss Code of Obligations (OR) 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 to be legally binding with a qualified electronic signature.

A certificate is only as trustworthy as the procedure that is used to create it. Swisscom (Schweiz) AG therefore divides certificates into "certificate classes". The higher the certificate class, the more extensive the identification checks involved in 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 documents to corroborate all of the information to be included on the certificate.

This CPS refers to all certificate classes, including the "qualified digital certificate", and meets the requirements of the Swiss Signatures Act.

1.1 Overview

This qualified CPS was drawn up by Swisscom (Schweiz) AG for the following purpose:

- To meet the requirements of a CSP of qualified certificates in accordance with ZertES [1]
- To meet the requirements of a CSP of advanced certificates in accordance with EIDI-V [8] and the associated implementation provisions [9]
- To describe the services, roles, limitations and obligations related to the use of qualified certificates issued by Swisscom Digital Certificate Services
- To guarantee interoperability in the use of qualified certificates issued by Swisscom Digital Certificate Services

The CPS is based on the guidelines set out in RFC 3647 [4].

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: 1.1
- Object identifier (OID): 2.16.756.1.83.2.1
- OID composition:

Position 1	Position 2	Position 3	Position 4	Position 5	Position 6	Position 7	Meaning
2							Joint ISO-CCITT Tree
	16						Country
		756					Switzerland
			1				Identifies organisation name (RDN)
				83			Swisscom Digital Certificate Services [1]
					2		Document framework Digital Certificate Services
						1	Certification Practice Statement (CPS)

[1] Issued by the Swiss Federal Office of Communications (OFCOM)

The OID assigned by OFCOM for the different categories can be found on the OFCOM Internet site under "RDN number" (relative distinguished number) (http://www.e-ofcom.ch).

1.3 Swisscom Digital Certificate Services participants

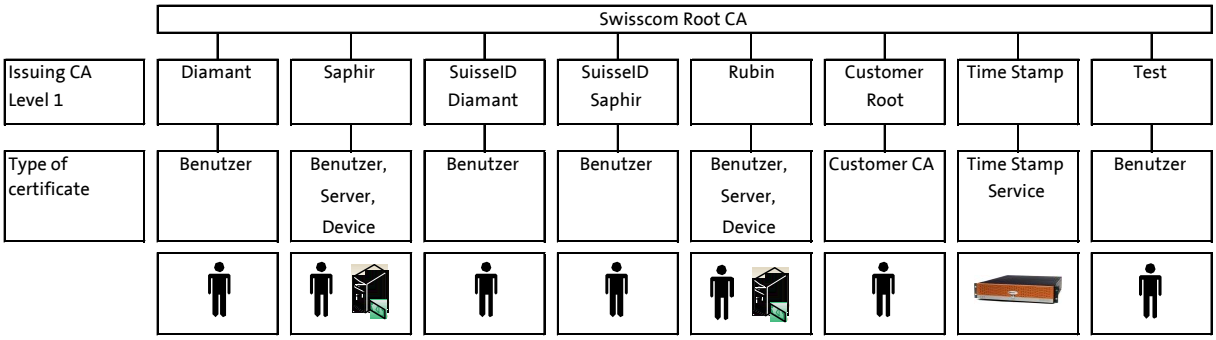
1.3.1 Certification Authorities (CAs)

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 which are directly downstream from Swisscom Digital Certificate Services.

Swisscom Digital Certificate Services has the following infrastructure:



1.3.1.2 Level 1 Certification Authorities (CAs)

The following Swisscom Digital Certificate Services certification authorities are operated downstream from the Root CA:

- **Diamond CA** (qualified): For issuing Diamond-class user certificates. Meets the requirements of ZertES. The certificate owner or subscriber uses a secure signature creation device (SSCD). The key is used for creating legally binding signatures. This level of certificate is only issued to natural persons, who nevertheless can represent legal entities. The certificate can only be used for signing purposes.
- **Diamond SuisseID CA** (qualified): For issuing Diamond-SuisseID-class user certificates. Meets the requirements of ZertES) and conforms the specification of SuisseID. The certificate owner or subscriber uses a secure signature creation device (SSCD). The key is used for creating legally binding signatures. This level of certificate is only issued to natural persons, who nevertheless can represent legal entities. The certificate can only be used for signing purposes.
- **Sapphire CA** (advanced): For issuing Sapphire-class user and device/server certificates. Conforms to the definitions set out in ZertES (article 2, clause B) for

advanced certificates 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 level of certificate is issued for natural persons and organisations and can be used for signing, encrypting and authenticating purposes.

- **Sapphire SuisseID CA** (advanced): For issuing Sapphire-SuisseID-class user and device/server certificates. Conforms to the definitions set out in ZertES (article 2, clause B) for advanced certificates and EIDI-V [8] and to the SuisseID specification. A secure signature creation device (SSCD) is used. This type of certificate is used for signatures in cases where there is no legal requirement for written form or for purposes which have been agreed by the parties. This level of certificate is issued for natural persons and legal entities and can be used for signing, encrypting and authenticating purposes.
- **Emerald CA:** For issuing Emerald-class user and device/server certificates. These are soft certificates and ***do not*** use a secure signature creation device (SSCD). Certificates from the Emerald CA are signed with a ValiCert Class 3 key by means of "RSA KEON ROOT SIGNING SERVICE" so that certificates issued from it are considered as "trusted" in the latest browsers and e-mail clients. Device certificates (SSL server/client) and certificates for e-mail security (sign and encrypt) are issued.
- **Ruby CA:** For issuing Ruby-class user and device/server certificates. These are soft certificates and ***do not*** use a secure signature creation device (SSCD). This level of certificate is issued for natural persons and organisations and can be used for signing, encrypting, authenticating, etc.
- **Customer CA:** For issuing digital CA certificates to create customer own Issuing CAs and to issue digital CA certificates to create a subordinate customer Root CA ( ). The private key to prepare a customer own Issuing CA is generated by SDCS through a HSM. The private key from the customer Root CA was generated and stored either in SSCD or in software.
- **TimeStamp CA:** For issuing certificates for the TimeStamp Service. Each TimeStamp Server has its own certificate.
- **Test CA:** For test purposes
- **E-RA-CA:** For issuing certificates for creating the SSL link between the Enterprise Registration Authority and the Trust Center. These certificates are only issued for E-RA officers and are bound to an SSCD.

The certification authorities issue certificates for users, organisations and devices. No other certification authorities are certified.

1.3.2 Registration Authorities (RAs)

The Swisscom (Schweiz) AG business model is based on a registration authorities (hereinafter RA) contractual partner model. Contractual partners of Swisscom (Schweiz) AG assume the role of RA. The RA partner is free to choose whether to issue certificates within its organisation only or to also act as a "public" RA.

RA partners are obliged by the terms of a Service Level Agreement (SLA) 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 one a year.

The Swisscom (Schweiz) AG business model differentiates the following types of RA:

- **Swisscom RA:** For issuing certificates for own use and downstream RAs (E-RA)
- ***E-RA*:** (Enterprise Registration Authority) is an RA partner authorised to create and issue SSCDs and certificates directly.
- ***TPS:*** (Trusted Point of Sale) is an RA partner which, as a registration authority, receives and checks the details of certificate applications. SSCDs for the "Diamond" and "Sapphire" certificate classes are personalised and distributed by an E-RA or a central distribution point.

A complete list of all public registration authorities is published on the web server referred to in section 2.2.

The identity check of subscribers is performed by employees of the registration authorities.

1.3.3 Subscribers

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

1.3.4 Relying parties

Information on relying parties is available in the respective CP.

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 acting on behalf of a subscriber or relying party, responsibility lies with the subscriber making the application.

Service provision agreements with a service provider or the acceptance of services from a service provider acting on its own behalf can only be concluded by the head of service of Swisscom Digital Certificate Services.

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 (Schweiz) AG
Digital Certificate Services
Müllerstrasse 16
8004 Zurich

The infrastructure described in section 1.3 is operated exclusively by Swisscom (Schweiz) AG.

1.5.2 Contact person

The person responsible for administering the CPS is the Engineering Manager of Digital Certification Services:

Swisscom (Schweiz) AG
Digital Certificate Services
Engineering Manager
Müllerstrasse 16
8004 Zurich

The Engineering Manager drafts the CPS in collaboration with Operations for the consultation process.

1.5.3 Persons responsible for the CPS

Overall responsibility for CPS content and compliance lies with the Governance Board. The Service Manager is responsible to the Governance Board for the correct provision of the CSP 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.

1.5.4 Approval procedure

Final approval of the CPS is made by the Governance Board. Other consultation bodies are the Chief Information Security Officer (CISO) and the Security Board.

1.5.5 Policy amendments

The guidelines may be amended at any time in accordance with the procedure described in section 1.5.4. If the amendments involve security-related aspects or affect the processes of the subscribers, the latter must be informed without delay.

The amended documents enter into force on the day they are published via the service described in section 2.2. An amendment to the CP/CPS is announced in the "News" section of the Swisscom Digital Certificate Services Internet site.

1.6 Terms and keywords

Term	Explanation
Certificate Service Provider (CSP) or Certification Authority (CA)	Authority which confirms information in an electronic environment and issues digital certificates for this purpose.
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 Swiss Federal Office for Metrology and Accreditation (METAS).
Certificate Practice Statement (CPS)	Statement on the rules and practices effectively applied by the CSP for issuing certificates. The CPS defines the devices, the policy and the procedures used by the CSP in accordance with its chosen certification policy.
Relying party	Person or process which relies on the verified electronic signatures when using a certificate.
Digital certificate	Electronic certificate that associates a signature verification key with the name of a person.
Electronic signature or signature	Data in electronic form that is added to or logically associated with other electronic data in order to authenticate such data.
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.

Term	Explanation
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.
Subscriber	Natural person who owns the signature key and who is assigned the signature verification key in the certificate.
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.
Qualified electronic signature	Electronic signature meeting the following requirements: 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 article 6, sections 1 and 2 of 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 article 7 of 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.
Key pair	Signature key and associated signature verification key which are mathematically linked by an asymmetrical signature algorithm.
Secure signature creation device (SSCD):	Device in accordance with article 6, section 2 of 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.
Trust Center	Special protected room where the CSP systems are operated

Term	Explanation
Certificate revocation	CSP service for revoking a certificate before it is due to expire
Certificate issuance	CSP service for making a generated certificate available to the subscriber and – if authorised by the subscriber – to other certificate users.
Certificate status management	CSP service which enables certificate users to check whether a certificate has been revoked.
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.
Certification authority (CA)	See "Certification services provider"
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.

Abbreviations

Term	*Explanation*
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
CN	Common name, as part of the DN
DN	Distinguished name in accordance with RFC 3739
ETSI	European Telecommunications Standards Institute
EIDI-V	Verordnung des EFD über elektronisch übermittelte Daten und Informationen (Provisions of the Federal Department of Finance (FEF) concerning electronically transmitted data and information).
GC Process	Business process of a Swisscom Group Company
HSM	Hardware Security Modules
LDAP	Lightweight Directory Access Protocol, repository service
LRA	Local Registration Authority (of an RA partner)
OCSP	Online Certificate Status Protocol
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)
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 certification services with regard to electronic signatures
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (Ordinance on Electronic Signatures, VZertES) of 3 December 2004
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Federal Act on Electronic Signatures) of 19 December 2003)

2 Publication and Repository Service

2.1 Repositories

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

- http://www.swissdigicert.ch, Menue item „Certificate“
- ldap://ldap.swissdigicert.ch/dc=swissdigicert, dc=ch

  The LDAP-DIP cuts into the following Certificate classes:

  - Valid CA classes:
    - Diamond CA
    - SuisseID Diamant CA
    - Sapphire CA
    - SuisseID Sapphire CA
    - Emerald CA
    - Ruby CA
    - Customer
- http access to CRL
  - http://www.swissdigicert.ch/download/sdcs-diamant.crl
  - http://www.swissdigicert.ch/download/sdcs-saphir.crl
  - http://www.swissdigicert.ch/download/sdcs-rubin.crl
  - http://www.swissdigicert.ch/download/sdcs-smaragd.crl
  - Etc.
- http access to OCSP:
  - http://ocsp.swissdigicert.ch/

2.2 Publication of certificate information

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

- Certificate and fingerprint of the Root CA of Swisscom Digital Certificate Services: http://www.swissdigicert.ch/sdcs/portal/page?node=download_ca
- CPS and CP: http://www.swissdigicert.ch/sdcs/portal/page?node=download_docs
- List of public registration authorities https://www.Swissdigicert.ch/index.mhtml/

- Information on the correct use of cryptographic material and a list of recommended applications

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 requested by the subscriber)
- Certificate revocation lists (CRL): at least every 24 hours
- 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. Write-access to this information is only available to authorised employees (see section 5.2).

Certificate information can only be retrieved by authorised users. E-mail addresses in particular are not supplied to non-registered users. Wildcard searches are not supported in the LDAP directory.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

Subscriber information is divided into two categories: required information and optional information. The following data needs to be recorded by the RA:

Data to be recorded	Diamond (qualified)	Sapphire (advanced)	Ruby/Emerald Sec. e-mail / server / device (advanced)

Required	• Subscriber's name:
	  ○ First name
	  ○ Middle name(s) where applicable
	  ○ Surname
	• Postal Address
	• Nationality (passport/ID card)
	• Document submitted
		• Subscriber's name:
		  ○ First name
		  ○ Middle name(s) where applicable
		  ○ Surname
		• Postal Address
		• Nationality (passport/ID card)
		• Document submitted
			• At least one person per organisation (field O= in DN) or domain (SSL server, e-mail) must be registered as in the case of Sapphire and guarantee that the details in the certificate are correct
			• For each domain

	• Period of validity of the document • Passport/ID number • Date of birth • Place of birth/citizenship • Proxy of legal person for certificate entry O= or OU=	• Period of validity of the document • Passport/ID number • Date of birth • Place of birth/citizenship • Proxy of legal person for certificate entry O= or OU=	entered in the certificate there must be one proxy of the legal person to which the domain refers
Optional	• E-mail address • Title (Dr., Prof.) • Pseudonym • Transaction amount (Standard = CHF 0.-) • Organisation name • Organisational Unit	• E-mail address • Title (Dr., Prof.) • Organisation name • Organisational Unit	• E-mail address • Organisation name • Organisational Unit • Fully qualified domain name for SSL Server • Application-specific details

Based on the very individual portion of the corresponding parameters the customer CA is deliberately not specified.

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

- CN=< Title, first name, middle name, surname, name of the organisation or of the device>
- C=< ISO Country Code DIN EN ISO 3166-1> If the subscriber does not have Swiss citizenship, the country code of the country, in which the subscriber's passport was issued (natural person) or the organisation is registered (legal entities)

[optional]

- S = <Surname>
- G = <Given name>
- O = <Organisation>
- OU = <Organisational Unit>
- L = <Locality>
- EMAIL = <E-mail address>
- PN = <Pseudonym>
- SN = <PID, AHV-Number, unique numerical identifier>
- SDA = <Date of birth>

Other attributes that can be recorded for the subscriber's name are listed in section 7.1.

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:

- *Data processing systems (not applicable for "Diamond")*
  The "common name" of data processing system should always contain the fully qualified domain name, e.g.: "cn=ldap.swissdigicert.ch".
- *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 entered 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.

- *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 (for qualified certificates)*
  The "common name" of a pseudonym begins with "PN:", e.g.: "cn=PN:Company Certificate".

The assignment of unique serial numbers is described in section 7.1.

3.1.3 Anonymity / pseudonymity

The rules in section 3.1.2 apply. Swisscom Digital Certificate Services and CA 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 recognition, authentication and role of trademarks are governed in the respective CP.

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 legal entity

Legal entities/organisations are authenticated during registration by submitting the appropriate legally binding documents (notarised commercial register extract, etc.).

3.2.3 Authentication of a natural person

The basic procedures for checking the identity of a natural person are set out in the respective CP. The authentication of a natural person requires a personal meeting with an employee from the registration authorities listed in section 1.3.2.
The following information is required:

- Surname, first name (middle name) and name affixes if they appear in the identification paper
- Postal address
- Type of identification paper, its number and issuing authority and period of validity

The following information is also required for issuing a certificate:

- E-mail address

  The E-Mail address must be verified during the registration process. The requester must prove that he has access to the mailbox and that he can use it to receive mail.

  An organization may contractually define that all certificates using the name of the organization in the „O"-field may only contain e-mail addresses in the „email"-field that are in the domain of the organization. Should such a contract exist, the organization takes full responsibility for the proper management of e-mail accounts. Therefore, the requirement to verify individual e-mail addresses during the registration process is optional.
- Authentication information (passphrase) for locking the certificate
- In the case of an organisation/organisation unit entry: Proof of association with the legal entity/organisation entered and a proxy for the legal entity

3.2.4 Non-verified information

Rules are set out in section 3.2.4 of in the respective CP.

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 in 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 blocking order is sent by post with details of the authorisation information
- Phone call from the RA responsible giving details of the authorisation information

- In exceptional circumstances a blocking order can also be issued via the CSP web portal. The subscriber is called back to verify his identity.

The contact details are contained in the lists of the authorised RAs.

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 in the respective CP.

4.1.2 Registration process

The RA partner can choose between decentralised and centralised variants of the registration process.

The registration of Diamond and Sapphire class certificates involves the following steps:

- The subscriber fills out an application
- The application and submitted documents are checked for completeness and correctness
- The DN is checked for uniqueness
- Identification papers and other official documents are scanned
- The scanned documents are archived in the Card Management System of Swisscom Digital Certificate Services and if necessary stored by the RA in a locked cabinet or on a suitably protected data system
- The information required for certification is sent to the certification authority via an encrypted data line with high-level authentication.
- The certificate request is digitally signed by the subscriber

In organisations which operate an E-RA, Ruby and Emerald certificates can also be delivered via automated interfaces or self-service portals provided it can be ensured that the details in the certificate are correct and authorised.

4.1.2.1 Decentralised SSCD distribution process

In the decentralised variant, the SSCDs are initialised by Swisscom and the key pair for the qualified signature is generated in a secure environment. The domain for the qualified keys is then blocked in the SSCD and the SSCD delivered to the LRA by secure means. At the LRA the data is registered and checked and the SSCD is then personalised. When the procedure has been concluded the applicant sets his personal PIN codes and is able to take the SSCD away with him.

4.1.2.2 Centralised SSCD distribution process

In the case of centralised delivery of the SSCD, the E-RA delivers the data (which was checked during a personal interview with the applicant at the RA) by secure means to a central office where the SSCD is first initialised and then personalised. The SSCD and the PIN letter with the transport PIN for activating the SSCD are sent to the subscriber separately. Once the card has been safely received via registered mail it can be activated and the cardholder needs to set his PIN code straight away.

4.2 Certificate application processing

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

4.2.1 Performing identification and authentication functions

Rules are set out in section 4.2.1 of in the respective CP.

4.2.2 Approval or rejection of certificate applications

Rules are set out in section 4.2.2 of in the respective CP.

4.2.3 Processing time

If the decentralised variant is used the applicant can take the SSCD away with him immediately. With the centralised variant, processing takes up to one week after certificate requests have been received.

4.3 Certificate issuance

"Diamond" and "Sapphire" class certificates are only issued on Swisscom (Schweiz) AG compliant SSCDs. The initialisation of the card and the generation of the qualified key pair on the card is performed in a secure environment by Swisscom Digital Certificate Services 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.

4.4 Certificate acceptance

4.4.1 Acceptance of the certificate

A certificate is deemed as accepted by the subscriber if

- the certificate is used or
- no objection is submitted within 10 days of receipt.

The rules in section 3.4 apply.

The issuing RA must immediately contact the CSP to revoke erroneously issued certificates.

4.4.2 Publication of the certificate

Certificates issued by Swisscom Digital Certificate Service are published by the repository service immediately after being issued, provided the certificate owner gives his consent.

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

Rules are set out in section 4.8 of in the respective CP.

4.9 Certificate revocation and suspension

Certificate revocation is described in the respective CP. The suspension of qualified certificates (Diamond) is not offered. The following rules apply to the Certificate Revocation List (CRL) (section numbering according to CP):

- (4.9.7) CRL issuance frequency: Updated CRLs are published at least once a day.
- (4.9.8) Maximum latency for CRLs: A new CRL is published as soon as a modification is made.
- (4.9.9) On-line revocation/status checking availability CRLs can be accessed via the URLs in section 2.1

4.10 Certificate status service

Swisscom Digital Certificate Services 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) by selecting the Zertifikatsabfrage menu. To query the status of a certificate enter surname (required) and first name (optional).
- 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) in the corresponding directory.

4.10.2 Service availability

The online status query via the Web Server and LDAP, and the CRL are available around the clock. Swisscom (Schweiz) AG provides a 99.99% availability guarantee for the LDAP service.

4.10.3 Optional features

Service availability is permanently monitored by Swisscom (Schweiz) AG. All important components necessary for providing the online status query via the Web Server and via LDAP are set up redundantly and support automatic switching in the event 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 by Swisscom Digital Certificate Services for signature keys. The same applies for "Sapphire" class certificates based on the regulatory requirements of EIDI-V.

Swisscom Digital Certificate Services offers RA partners a procedure for generating encryption keys for the Ruby and Emerald certificate classes outside an SSCD, which can be stored in an appropriate manner so as to allow them to be recovered.

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 [4].

Some areas may be dealt with in separate documents, which may or may not have been 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 (Schweiz) AG. Important components are set up redundantly and are located in two separate computing centers. The buildings housing the two computing centers are far enough apart to prevent them from both being affected by natural disasters or catastrophes. The buildings are in Bern and Zurich.

The rooms provide sufficient protection in terms of infrastructural security and comply with the provisions of ZertES [1], TAV [3] and the referenced documents, in particular ETSI TS 101 456 [5].

5.1.2 Access controls

The operating rooms of the CSP 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 data center of the CSP is protected by an access system which uses a biometric recognition procedure.

5.1.3 Power and air conditioning

The CSP data center 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

The following media storage devices are used:

- Paper
- CD-ROM
- USB storage modules
- Hard disks
- Hardware Security Modules (HSM)
- Secure Signature Creation Devices (SSCD)

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

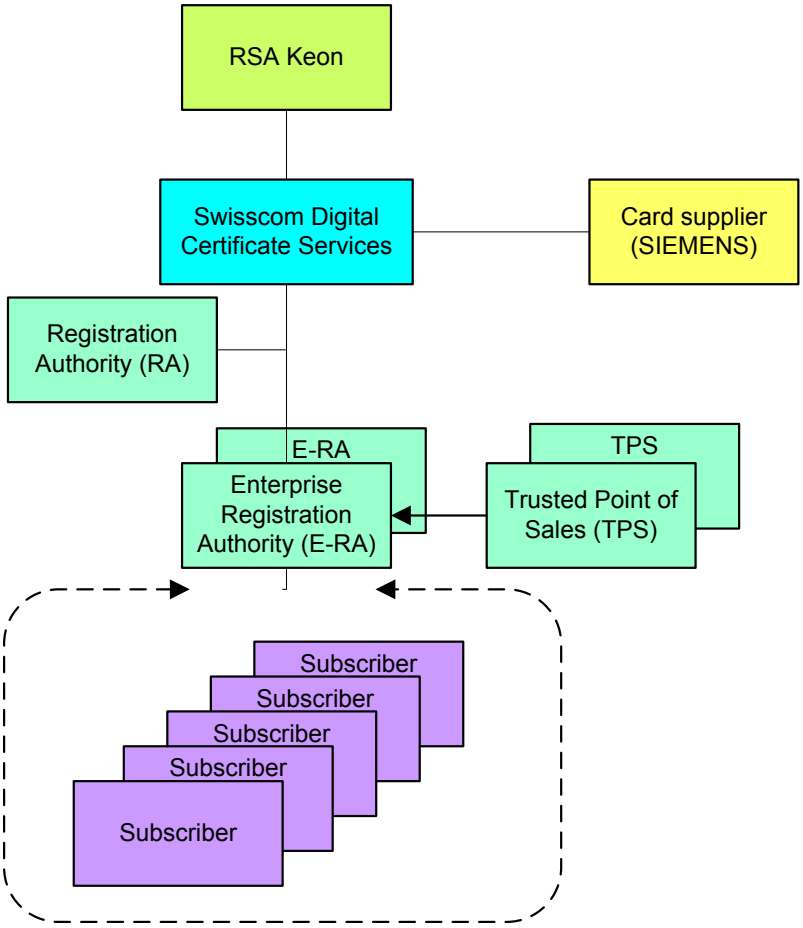
The critical components for safeguarding interruption-free operation are split between two computing centers. The backups of computing center 1 are stored in computing center 2. The two computing centers are 30km apart.

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

The division of roles at Swisscom Digital Certificate Services provides for the outsourcing of registration activities to suitable external service providers. Other dependencies arise from its own certification as a CSP of qualified certificates and delivery by card manufacturers.



This results in the following role distribution:

Description	Role	Task
RSA Security	Supplier	• Authorises the Trust Center to sign its own RSA-Keon certificates • Supply of backend systems (CA)
Siemens	Supplier	• Supply of secure signature creation devices (SSCD) to the CSP
SafeNet	Supplier	• HSM for CA • Time stamp appliance
Authentidate	Supplier	• Time stamp software
Meinberg	Supplier	• GPS time server appliance
Intercede	Supplier	• Certificate Management System and RA Front End

Description	Role	Task
Swisscom Digital Certificate Services CSP	Certificate Authority	• Provision of infrastructure, structure and workflow management for the certification service • Pre-personalisation of the secure signature creation devices • Delivery of pre-personalised signature creation devices to the registration authority (RA) • Creation and administration of certificates • Provision of basic infrastructure for RA • Provision of services for signature/certificate checks and time stamping • Contact point for RA queries • Contact point for misuse/fraud reports
Enterprise-Registration Authority Registration authority of a contract partner (E-RA/TPS)	Registration authority for certificate requests	• Registration and forwarding of applications and personal details of the subscriber • Personalisation and issuing of secure signature creation devices • Contact point for subscriber issues
Subscriber	Owner of a certificate issued by Swisscom Digital Certificate Services	• Certificate request (can also be delegated to a Trusted Point of Sales) • Receipt of secure signature creation devices from the registration authorities • Use of the provided certification services • Request for certificate revocation
Relying party	Third person who checks the signature of a subscriber	• Queries the authenticity and validity of a signature created by a subscriber or the subscriber's certificate at the Trust Center

Registration authority (RA)

Although Digital Certificate Services outsources the registration of subscribers to an RA partner (E-RA/TPS) it does operate its own RA for the registration of LRA Officers and internal Swisscom requirements. As a superordinate registration authority, the Swisscom RA is able to view all entries of the various E-RAs and if necessary can also revoke certificates issued by E-RAs.

The Swisscom RA is operated by the RA Administrator.

RA Partner (E-RA)

Digital Certificate Services outsources the registration of subscribers to RA partners (E-RA). The E-RAs assume responsibility for the correct registration and vetting of the subscriber's personal identification details and attributes required for the creation and issuing of certificates, and the personalisation of secure signature creation device (SSCD). The RAs transfer this information to the Trust Center, where the certificate is issued.

The RAs are responsible for the organisational structure and role concept. Basic roles (administrators, vettors, auditors) are filled at all RAs, although the composition of the roles may vary.

Trusted Point of Sales (TPS)

A Trusted Point of Sales (e.g. the HR department of a company) applies to the RA for certificates for multiple subscribers (e.g. employees of a company), for which it collects the required identification data and attributes and forwards to the RA. The Trusted Point of Sales is responsible for clearly identifying the subscriber and the accuracy of the collected data.

A Trusted Point of Sales endeavours to provide complete and accurate information about the subscribers and to handle the secure signature creation devices and key pairs it is entrusted with extreme care until delivery to the subscriber. Employees at the Trusted Point of Sales may only use the key pairs they have been assigned for the specific purpose of processing the application.

External service providers & suppliers

The Trust Center uses RSA Keon software for RSA Security, Intercede MyID for Certificate Management and RA Front-End and Sun Java Directory for the LDAP repository service. The secure signature creation devices (SSCD) are supplied by Siemens, the HSM and Timestamp Appliance by SafeNet, the Timeserver by Meinberg and the Timestamp Software by AuthentiDate.

Subscribers

Each subscriber in turn undertakes to provide the registration authority with complete and accurate information about his person, to handle the secure signature creation device he is assigned with extreme care and to only use it in accordance with the Certificate Policy.

In the event of the private key being lost or compromised the RA and the subscriber must arrange for the certificate to be revoked at the earliest opportunity.

5.2.1.1 Role concept of the Trust Center

The role concept of the Trust Center is based on the business processes. These are depicted in figure 1 (Group Company Processes):

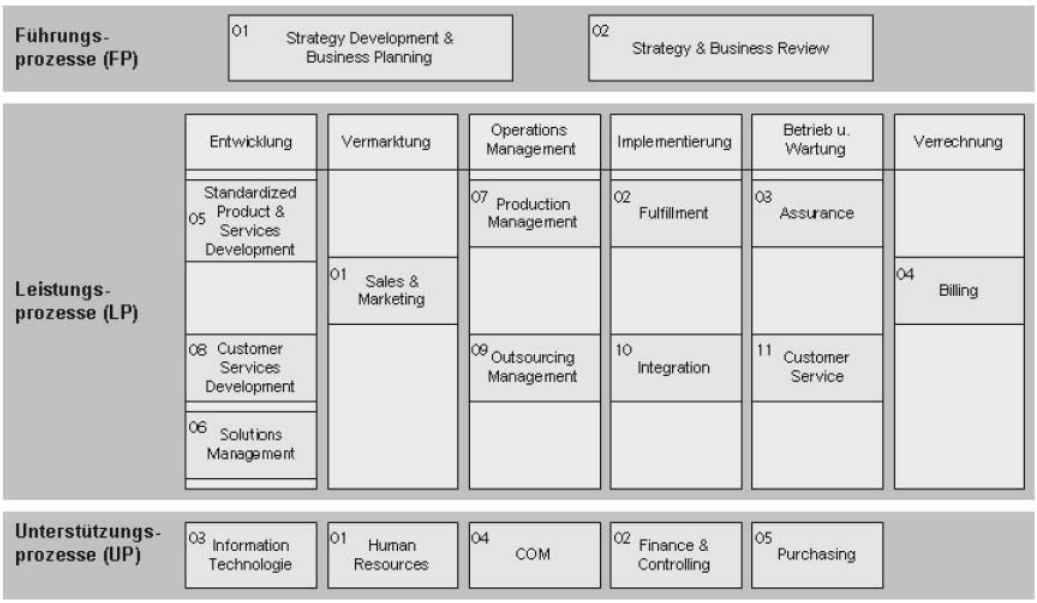


Fig. 1: Group Company Processes 1

The associated organisation structure of the Trust Center with the assignment of the relevant business processes is as follows:

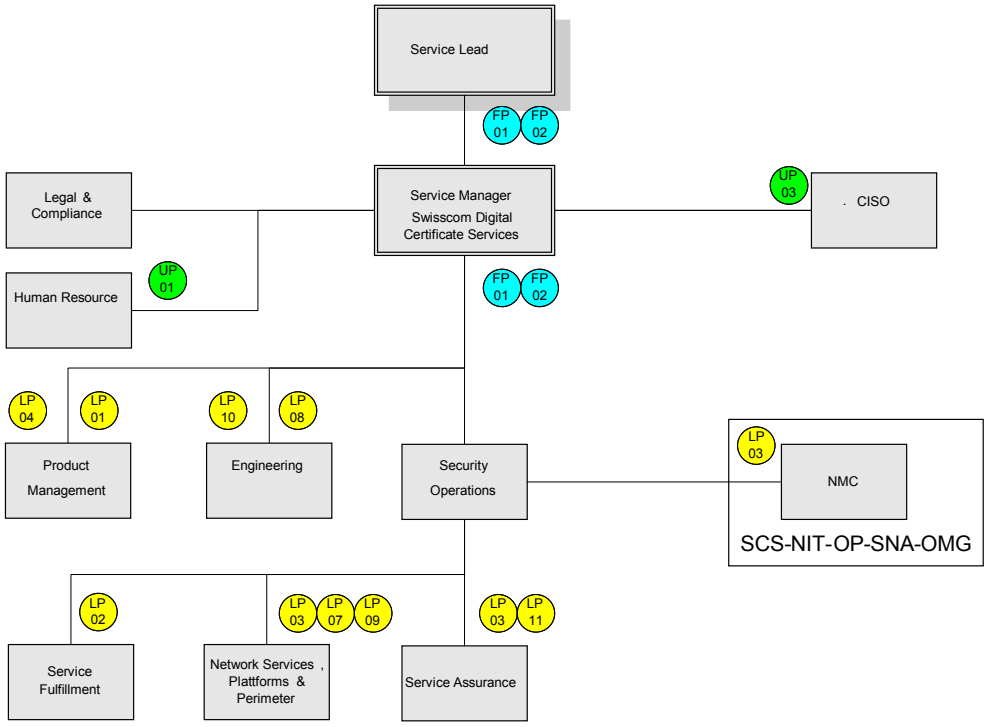


Abb. 2: Organisation of the Trust Center 1

Roles and competencies are assigned in accordance with the respective responsibilities of the GC Processes.

A simple relationship exists between the GC-specific processes – Management, Service and Support processes – and the roles required for Digital Certificate Services, as can be seen in the following table:

No	GC-specific process	Organisational Unit	Role(s)
FP01	Strategy Development & Business Planning	System Integration	Service Lead Service Manager Legal & Compliance (only indirectly)
FP02	Strategy & Businesss Review	System Integration	Service Lead Service Manager
LP01	Sales & Marketing	ICT Security Solutions	Product Manager Legal & Compliance (only indirectly)
LP02	Fulfilment	Service Fulfilment	Procurement Manager
LP03	Assurance	Security Operation Center	2nd Level Support 3rd Level Support Perimeter Administrator Perimeter Engineer
		Service Assurance	1st Level Support Building Security
		Swisscom Fixnet – NMC	Building Security
LP04	Billing	ICT Security Solutions	Product Manager
LP05	Standardized Product & Service Development	n/a	n/a
LP06	Solutions Management	n/a	n/a
LP07	Production Management	Systems & Platforms	Head of Security Operation
		Miscellaneous	Root CA Key Holder

No	GC-specific process	Organisational Unit	Role(s)
		Security Operation Center	Root CA Administrator Root CA Operator TSA Administrator TSA Operator System Administrator System Operator RA Administrator CA 2nd Level Support CA 3rd Level Support
		Head of SOC	Change Manager Configuration Manager Crisis Manager / BCP Manager
		Diverse	Change Advisory Board
		Swisscom Fixnet - NMC	Building Security Binzring 17
		Service Assurance	Building Security RZ Bern
LP08	Customer Services Development	ICT Security Solutions	Engineering Manager
LP09	Outsourcing Management	Systems & Platforms	Head of Security Operation
LP10	Integration	n/a	n/a
LP11	Customer Service	Service Assurance	1st Level Support (helpdesk)
UP01	Human Resource	Human Resource	Human Resource
UP02	Finance & Controlling	Finance & Controlling	Finance & Controlling
UP03	Information Technology	Diverse SCSL-Abteilungen	Security Board
		ICT Security Solutions	Security Officer Information Security Officer
UP04	COM	n/a	n/a
UP05	Purchasing	n/a	n/a

The roles listed in the above table are required for the implementation and provision of the services. In the following list, the various roles are grouped according to function. A person can

have several roles. However, multiple roles may not be permitted or not possible because of the need to keep certain functions separate (cf. 5.2.4).

Management and supervisory roles:

- Service Head (SH)
- Service Manager (SM)
- Product Manager (PM)
- Engineering Manager (EM)
- Security Board (SB)

TRUST CENTER operational roles:

- Security Operation
  - Head of Security Operation (OM)
  - Root CA Administrator (RCAD)
  - Root CA Operator (RCOP)
  - TSA Administrator (TAD)
  - TSA Operator (TOP)
  - System Administrator (SAD)
  - System Operator (SOP)
  - RA Administrator (RAAD)
  - 1st Level Support (1LS)
  - 2nd Level Support (2LS)
  - 3rd Level Support (3LS)
- Special roles
  - Change Manager (CM)
  - Change Advisory Board (CAB)
  - Crisis Manager / BCP Manager (CM)
  - Crisis Team / Business Continuity Team (BCT)
  - Configuration Manager (CM)
  - Procurement Manager (PRM)
- Perimeter Monitoring Roles
  - Celeris Administrator (CAD)
  - Perimeter Security Engineer (PSE)
- Building Security (partly outsourced to Swisscom Fixnet) (GB 1and GB2)
- IT Call Center

Other roles have a supporting function for the implementation, maintenance and monitoring of the Trust Center's workflow management:

- Chief Security Officer (CSO)
- Chief Information Security Officer (CISO)
- Information Security Officer (ISO)
- Legal & Compliance (LC)
- Human Resources (HR)
- Internal Audit (IA)

5.2.2 Employees involved in the various procedures

The following table describes security-related activities and their corresponding roles. The table also shows which activities require the four-eyes principle.

Activity	Role	4-eyes principle
Operation of the Trust Center		
Publication of certificates and revocation lists	RCAD RCOP	
Key escrow of private CA keys for self-operated CAs (not for Diamond certificates)	RCAD with ISO	x
Input of boot and administration passwords for cryptographic devices without TSA	RCAD with ISO	x
Input of boot and administration passwords in general	SAD SOP	x
Starting and stopping of processes on cryptographic devices	RCAD RCOP	x
Input of boot and administration passwords for TSA	TAP TOP	
Starting and stopping of TSA processes	TAD TOP	x
Starting and stopping of processes involving non-cryptographic components	SAD SOP	
Input of new releases, upgrades, patches on cryptographic devices without TSA	RCAD RCOP ISO	x
Input of new releases, upgrades, patches on TSA	TAD TOP ISO	x
Input of new releases, upgrades, patches on non-cryptographic Trust Center Systems	SAD SOP	x
Data security/backup of and re-inputting on cryptographic devices without TSA	RCAD RCOP	x

Activity	Role	4-eyes principle
Operation of the Trust Center		
Data security/backup and re-inputting on TSA	TAD TOP	x
Data security/backup or re-inputting in general (non-cryptographic devices)	SAD SOP	x
Generation of root CA keys	RCAD RCOP ISO OM	8-eyes principle
Generation of CA keys	RCAD RCOP ISO	x
Checking the log files of cryptographic devices	RCAD RCOP ISO IR	x
Security monitoring of the network	CAD PSE	
Issuing of access rights	HR	
Issuing of access rights in general	SAD	x

5.2.3 Identification and authentication of roles

The identification and authentication of roles is based on the role models described in the previous sections. 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 Root CA Administrator and the ISO. All access is based on the "4-eyes-principle".

Physical access to the individual IT systems is regulated by access control mechanisms.

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. The special function of Key Holder is not listed as this is covered by several roles. When dividing role functions between employees, care must be taken to ensure that an individual is not assigned incompatible roles.

Incompatible with	**Administration/Management**	Service Head	Service Manager	Product Manager	**Conception**	Engineering Manager	**Configuration and Operation**	Head of Operations	Root CA Administrator	Root CA Operator	System Administrator	System Operator	TimeStamp Operator	RA Administrator	CA 1st Level Support	CA 2nd Level Support	CA 3rd Level Support	Change Manager	Change Advisory Board	Crisis Manager	Configuration Manager	Procurement Manager	Building Security Binzring 17	Building Security RZ Bern	Celeris Administration	Perimeter Security Engineer	IT Call Center	**Monitoring**	Security Board	Information Security Officer	Security Officer	Internal Audit	**Other**	Legal & Compliance
Administration/Management																																	
Service Head																																	
Service Manager																																	
Product Manager																																	
Conception																																	
Engineering Manager																																	
Configuration and Operation																																	
Head of Operations																																	
Root CA Administrator																																	
Root CA Operator																																	
System Administrator																																	
System Operator																																	
TimeStamp Operator																																	
RA Administrator																																	
CA 1st Level Support																																	
CA 2nd Level Support																																	
CA 3rd Level Support																																	
Change Manager																																	
Change Advisory Board																																	
Crisis Manager																																	
Configuration Manager																																	
Procurement Manager																																	
Building Security Binzring 17																																	
Building Security RZ Bern																																	
Celeris Administration																																	
Perimeter Security Engineer																																	
IT Call Center																																	
Monitoring																																	
Security Board																																	
Information Security Officer																																	
Security Officer																																	
Internal Audit																																	
Other																																	
Legal & Compliance																																	
Human Resources																																	

5.3 Personnel security controls

5.3.1 Requirements of all employees

Swisscom Digital Certificate Services 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,

- Unix operating systems, TCP/IP networks and LDAP.

5.3.2 Background checks for employees

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

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

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

5.4 Security monitoring

5.4.1 Monitored events

The following measures have been adopted 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 certification authority 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 CISO, 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 CISO.

5.5 Archiving

5.5.1 Archived data

Data related to the certification process is archived:

- Certificate entries containing personal information about the subscriber
- 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", TimeStamp and Test, including the associated private keys
- Contracts

- Activity journal of Swisscom Digital Certificate Services
- Devices and applications for reading and representing the archived data

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 different data centers.

5.5.5 Time stamping requirement

The requirements in ZertES and TAV[3] apply.

5.5.6 Archiving system

An internal archiving system is used.

5.5.7 Procedures for obtaining and verifying archived data

The CISO 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 compromisation

The procedures for handling security incidents and the compromisation 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.

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 Compromisation of private keys of the certification authority

If the private key of the certificate authority has been compromised, or there is justified suspicion of a compromise, the Security Board of the CA 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 so as to prevent incorrect or invalid statements being issued by the service.
- Generation of a new key pair and a certificate for the certification authority.
- Publication of the certification authority's 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 space 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

The conditions for terminating business operations are set out in Art. 13 ZertES, Art. 10 VZertES and section 7.4.9 ETSI 101 456 [5]. A summary of the conditions of ZertES and VZertES was published by METAS in the document "Interpretationen zu den Fragen im Zusammenhang mit der Anerkennung von CSP im Bereich der elektronischen Signature (Interpretation of issues concerning the accreditation of CSP in the field of electronic signatures)" (No. 518.d, March 2005, Rev.00). Based on this, Digital Certificate Services needs to implement the following regulations:

- Swisscom Digital Certificate Services informs SAS/METAS. SAS commissions another CSP to manage the repository and activity journal and to store the respective supporting documents (Art. 13 ZertES).

- Swisscom Digital Certificate Services must be in a position to provide phase plans for the transfer of its operations to another CSP and for taking over the operations of another CSP. The phase plan for terminating business operations must include the following definitions and descriptions:
    - An asset list of the CSP (list of HW & SW components, location, details of the format of the stored data
    - Conditions of the scope of application
    - A summary of the telephone numbers and functions of the main contact partners
    - An account of the communication channels, i.e. an overview of the people or offices that need to be officially informed internally and externally
    - A detailed description of which information needs to be distributed to subscribers and authorities (letters, press releases). It should also be remembered that information needs to be sent to the local registration authorities and the Trusted Points of Sale.
    - A Re-Engineering Plan, i.e. a flow chart or phase plan showing which steps are involved in the migration of the qualified certificates to the new CSP
    - A timetable indicating the time phases (weeks, months) during which migrations will take place between the new CSP and terminated CSP

ETSI 101 456 [5] provides summaries of and supplements to the above requirements:

- Digital Certificate Services must revoke all rights issued to the registration authorities and Trusted Points of Sale and perform certification authority functions on their behalf
- Digital Certificate Services must hand over registration information and event log archives for the "period of production" involving subscribers and relying parties to the new CSP.
- Digital Certificate Services must have taken provisions to ensure that the costs of fulfilling the termination conditions are fully covered – even in the event of bankruptcy

If certification operations are to be terminated, the following measures must be taken:

- Inform the certification authority and SAS/METAS
- 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.

In the event of Swisscom (Schweiz) AG going bankrupt, Digital Certificate Services may be sold.

6 Technical security controls

The technical security requirements of a CSP or 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 17799.

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 backed up 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 legislation (ZertES) and are conform at least to FIPS 140-2 Level 3.

6.1.2 Private key delivery to subscriber

Encryption certificates are generated in accordance with the customer's security requirements. 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. These requirements are worked out on a project basis as part of a security concept.

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 (c.f. 2.1).

6.1.5 Key sizes

The cryptographic algorithms used and their key lengths are based on the ETSI [ETSI TS 102 176-1 V1.2.1 (2005-07)] publications referred to in TAV [3] and are currently:

- RSA 4096 SHA-1 for the CA 1 Root Key
- RSA 2048 SHA-1 for the CAs of the next level (Level 1) with the identifier CA 1
- RSA 2048 SHA-1 for advanced and timestamp (Sapphire, Ruby, Timestamp) with the identifier CA 1
- RSA 4096 SHA-256 for the CA 2 Root key
- RSA 4096 SHA-256 for the CAs of the next level (Level 1) with the identifier CA 2
- RSA 4096 SHA-256 for advanced and timestamp (Sapphire, Ruby, Timestamp) with the identifier CA 2

The RSA ROOT SIGNING Service for Emerald certificates uses the RSA 1024 SHA-1 key for the ValiCert Class 3 Policy Validation Authority (Trusted Root) and the RSA Public Root CA v1 which signed the CA Emerald certificate.

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) (c.f. 7.1.2) and are contained in the respective CP.

6.2 Private key protection

The private key of the root CA and CAs of the next level (Level 1) 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 an SSCD. Signatures are processed in the SSCD. The SSCD used meets the requirements of TAV [3] 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 CA3 / SA

- FIPS 140-1 Level 3

SSCD: Siemens CardOS 4.3B

- CC EAL4 +

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 SSCD and there is no possibility of the signature key being used outside the SSCD.

Copies of the key pairs of the Root CA and CA Services 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 Private key transfer to a cryptographic module

"Diamond" and "Sapphire" class signature and authentication keys and CA keys are only created in cryptographic modules (HSM and Smart Cards).

6.2.7 Private key storage on cryptographic module

"Diamond" and "Sapphire" class signature and authentication keys and CA keys are only stored in cryptographic modules (HSM and Smart Cards).

6.2.8 Method of activating private key

"Diamond" and "Sapphire" class private keys are activated by entering activation data (e.g. PIN). The black PED key is used for activating CA Level 1 private keys of the certification authority. This PED key is held by the "RCOP" role. Activation can only take place in the presence of a second person (four-eyes-principle).

6.2.9 Method of deactivating private key

6.2.10 Method of destroying private key

The four-eyes principle is applied when destroying private keys of the Root CA and the certification authorities it operates. Destroying the keys is the responsibility of the CISO and RCAD roles.

6.2.11 Cryptographic module rating

See 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:

- Root certificate of the Root CA, up to 20 years
- Certificates of downstream Level 1 CAs, up to 10 years
- "Emerald" class CA certificates signed by RSA, up to 2 years
- "Diamond", "Sapphire" and "Ruby" class certificates, up to three (3) years
- "Emerald" class certificates, up to 1 year

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 (see section 6.1.5).

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 generation and installation

Not applicable.

6.4.2 Activation data protection

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.

6.4.3 Other aspects

Swisscom (Schweiz) AG publishes instructions and recommendations on the Internet site http://www.swissdigicert.ch explaining which applications or procedures should be used for created signatures that meet the requirements of the "qualified" classification.

If these instructions are not followed the signature will not be classed as qualified.

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 (see also section 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 TAV [3] 3.5 requirements. 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 stamping service is provided by a SafeNet Luna TS appliance. The time stamp appliance is operated at Level 1, the same as the CA's HSM. 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 ZertES [1], TAV [3] and the referenced documents, in particular ETSI TS 101 456 V1.2.1 [4] and set out in the CPS.

7.1 Certificate profiles

The following required fields are available, as defined in the X.509 v3 standard and in accordance with TAV [3]:

7.1.1 Root CA 1 certificate

X.509 field	Value, OIDs	Comments
Version	2,	Version 3
serialNumber	xxxxxx	Number [integer]
signature		
algorithm	{1 2 840 113549 1 1 5}	sha1WithRSAsignarure
Issuer	CN=Swisscom Root CA 1 O=Swisscom OU=Digital Certificate Services C=CH	DirectoryString, UTF8String
Validity		
notBefore	" YYMMDDHHMMSSZ ",	UCT, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ " },	UCT, ETSI TS 102 280
Subject	CN=Swisscom Root CA 1 O=Swisscom OU=Digital Certificate Services C=CH	DirectoryString, UTF8String
subjectPublicKeyInfo		
Algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
subjectPublicKey	'........'B },	4096 Bit, BIT STRING

Extensions		
authorityKeyIdentifier		
subjectKeyIdentifier		
keyUsage	keyCertSign, cRLSign, DigitalSignature	
Critical	TRUE,	BOOLEAN
basicConstraints {		
extnValue	CA TRUE	
PathLenConstrains	7	
PolicyMappings		
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 0 1 } },	In a CA certificate, these policy information terms limit the set of policies for certification paths which include this certificate.

7.1.2 Root CA 2 certificate

X.509 field	Value, OIDs	Comments
Version	2,	Version 3
serialNumber	xxxxxx	Number [integer]
signature		
algorithm	{1 2 840 113549 1 1 11}	SHA256withRSA
Issuer	CN=Swisscom Root CA 2, O=Swisscom, OU=Digital Certificate Services C=CH	DirectoryString, UTF8String
Validity		
notBefore	" YYMMDDHHMMSSZ ",	UCT, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ " },	UCT, ETSI TS 102 280
Subject	CN=Swisscom Root CA 2, O=Swisscom, OU=Digital Certificate Services, C=CH	DirectoryString, UTF8String
subjectPublicKeyInfo		
Algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
subjectPublicKey	'........'B },	4096 Bit, BIT STRING

Extensions		
authorityKeyIdentifier		
subjectKeyIdentifier		
keyUsage	keyCertSign, cRLSign, DigitalSignature	
Critical	TRUE,	BOOLEAN
basicConstraints {		
extnValue	CA TRUE	
PathLenConstrains	7	
PolicyMappings		
certificatePolicies {		
extnId	{ 2 5 29 33 },	
extnValue	{ 2 16 756 1 83 2 1 } },	In a CA certificate, these policy information terms limit the set of policies for certification paths which include this certificate.

7.1.3 Qualified certificate (Diamond) CA 1

X.509 field	Value, OIDs	Comments
version	2,	Version 3
serialNumber	xxxxxxx	1 or another whole number [integer]
signature {		
algorithm	{1 2 840 113549 1 1 5}	sha1WithRSAsignarure
parameters	NULL },	
issuer	{ "CN=Swisscom Root CA 1, O=Swisscom, OU=Digital Certificate Services, C=CH" },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UCT, ETSI TS 102 280

X.509 field	Value, OIDs	Comments
notAfter	" YYMMDDHHMMSSZ " },	UCT, ETSI TS 102 280
subject	{ "CN=Swisscom Diamond CA 1, O=Swisscom, OU=Digital Certificate Services, C=CH },	directoryName, UTF8String
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	
subjectPublicKey	'.....'B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subjectPublic-Key-BitString of "Root CA 1"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subjectPublicKey-BitString of "Q-CA 1"
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000110000`B },	keyCertSign, cRLSign
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 2 1 } },	In a CA certificate, these policy information terms limit the set of policies for certification paths which include this certificate.
issuerAltName {		
extnId	{ 2 5 29 18 },	
extnValue	{ "O=ZertES-Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA" } },	directoryName, UTF8String
basicConstraints {		
extnId	{ 2 5 29 19 },	
critical	TRUE,	BOOLEAN
extnValue	{ cA TRUE },	BOOLEAN
pathLenConstraint	0 },	INTEGER, no other CA darunter
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	"http://www.swissdigicert.ch/download/Swisscom Digital Certificate Services-root.crl" },	[uRI], IA5String
AuthorityInfoAccess{		SEQUENCE{
extnId	{ 1 3 6 1 5 5 7 1 1 },	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessMethod	{ 1 3 6 1 5 5 7 48 2 },	id-ad-caIssuers
accessLocation	"http://www.swissdigicert.ch/download"},	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
	"http://ocsp.swissdigicert.ch"	[uRI], IA5String

X.509 field	Value, OIDs	Comments
accessLocation	}}},	
qcStatements {		
extnId	{ 1 3 6 1 5 5 7 1 3 },	
critical	TRUE,	BOOLEAN
extnValue	SEQUENCE OF {	OCTET STRING
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 1 }}}}}	qcs-QcCompliance
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 5},	sha1WithRSAsignarure
parameters	NULL },	
signature	`...... `B }	2048 Bit, BIT STRING

7.1.4 Qualified user certificate (Diamond) CA 1

X.509 field	Value, OIDs	Comments
Version	2,	Version 3
serialNumber	Unique Integer > 1000	[Integer]
signature {		
algorithm	{1 2 840 113549 1 1 5}	sha1WithRSAsignarure
parameters	NULL },	RFC 3279
Issuer	{ "CN=Swisscom Diamond-CA 1, O=Swisscom, OU=Digital Certificate Services, C=CH},	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UCT, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ " },	UCT, ETSI TS 102 280
Subject	-- obligatory {" S=Surname, G=Given name and middle name CN = Given name Middle name Surname *or* PN=Pseudonym, C=Country, -- optional O= ,OU= , E=EMail, Title, Place of birth, AHV-No "},	directoryName, UTF8String, ETSI TS 102 280
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	RFC 3279
subjectPublicKey	'.........'B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subjectPublic-Key-BitString of "Q-CA 1"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subjectPublicKey-BitString of this subject/end entity"
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000010`B },	nonRepudiation

X.509 field	Value, OIDs	Comments
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 2 2 } },	In an end entity certificate, these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.
issuerAltName {		
extnId	{ 2 5 29 18 },	
extnValue	{ "O=ZertES-Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA" }},	directoryName, UTF8String
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	"ldap://ldap.swissdigicert.ch/CN=Swisscom Diamant CA 1,dc=diamond,dc=swissdigicert,dc=ch?certificateRevocationList? , http://www.swissdigicert.ch/download/Swisscom Digital Certificate Services-diamat.crl"},	[uRI], IA5String
AuthorityInfoAccess{		SEQUENCE{
extnId	{ 1 3 6 1 5 5 7 1 1 },	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessMethod	{ 1 3 6 1 5 5 7 48 2 },	id-ad-caIssuers
accessLocation	"http://www.swissdigicert.ch/download"},	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	"http://ocsp.swissdigicert.ch/diamant" }}},	[uRI], IA5String
qcStatements {		
extnId	{ 1 3 6 1 5 5 7 1 3 },	
extnValue	SEQUENCE OF {	OCTET STRING
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 1 }},	qcs-QcCompliance
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 2 },	qcs-QcLimitValue
statementInfo	SEQUENCE {	MonetaryValue
currency	CHF,	Iso4217CurrencyCode
Amount	2,	CHF 0-2 Mio
exponent	6 }}},	INTEGER
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 4 }}}}}	qcs-QcSSCD
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 5},	sha1WithRSAsignarure
parameters	NULL },	RFC 3279
signature	`...... `B }	2048 Bit, BIT STRING

7.1.5 User certificate (Saphire) CA 1 for authentication

X.509 field	Value, OIDs	Comments
Version	2,	Version 3
serialNumber	Unique Integer	[Integer]
signature {		
algorithm	1 2 840 113549 1 1 5	sha1WithRSAsignarure

X.509 field	Value, OIDs	Comments
parameters	NULL	RFC 3279
Issuer	CN=Swisscom Saphire CA 1, O=Swisscom, OU=Digital Certificate Services, C=CH	directoryName, UTF8String
validity {		
notBefore	YYMMDDHHMMSSZ	UCT, ETSI TS 102 280
notAfter	YYMMDDHHMMSSZ	UCT, ETSI TS 102 280
Subject	-- obligatory CN=Surname, Given name or company, Organisation, Acronym *or* PN=Pseudonym, C=Country, E=name@provider.ch, C=Land -- optional O= ,OU= , Title, SN=Date of birth, L=Place of bith,	directoryName, UTF8String, ETSI TS 102 280
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	RFC 3279
subjectPublicKey	'.....'B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subjectPublic-Key-BitString of "Q-CA 1"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subjectPublicKey-BitString of this subject/end entity"
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000001`B },	digitalSignature
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 3 } },	In an end entity certificate, these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.
issuerAltName {		
extnId	{ 2 5 29 31 },	
extnValue	"ldap://ldap.swissdigicert.ch/CN=Swisscom Saphire CA 1 dc=saphire,dc=swissdigicert,dc=ch?certificateRevocationList? , http://www.swissdigicert.ch/download/sdcs-saphire.crl"},	[uRI], IA5String
extKeyUsage {		
extnId	{ 2 5 29 37 },	
extnValue	{1 3 6 1 5 5 7 3 4}, {1 3 6 1 5 5 7 3 2}},	E-Mail protection, clientAuth
		SEQUENCE{

X.509 field	Value, OIDs	Comments
AuthorityInfoAccess{		
extnId	{ 1 3 6 1 5 5 7 1 1 },	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE	
accessMethod	{ 1 3 6 1 5 5 7 48 2 },	id-ad-caIssuers
accessLocation	"http://www.swissdigicert.ch/"}	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	"http://ocsp.swissdigicert.ch/sahpir)" }}},	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 5},	sha1WithRSAsignarure
parameters	NULL },	RFC 3279
signature	`..... `B }	2048 Bit, BIT STRING

7.1.6 User certificates (Ruby and Emerald) CA 1 for secure e-mail, encryption, authentication

X.509 field	Value, OIDs	Comments
Version	2,	Version 3
serialNumber	Unique Integer	[Integer]
signature {		
algorithm	{1 2 840 113549 1 1 5}	sha1WithRSAsignarure
parameters	NULL },	RFC 3279
issuer	CN=Swisscom Smaragd (Rubin)-CA 1, O=Swisscom, OU=Digital Certificate Services, C=CH	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UCT, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ " },	UCT, ETSI TS 102 280
subject	{"CN=Given name Family name or Company, Organisation and E=name@provider.ch, C=Country, -- optional O= ,OU= , , SN=Date of birth, L=Place of birth "},	directoryName, UTF8String, ETSI TS 102 280
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	RFC 3279
subjectPublicKey	`........`B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subjectPublic-Key-BitString of "Q-CA 1"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subjectPublicKey-BitString of this subject/end entity"
keyUsage {		

X.509 field	Value, OIDs	Comments
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000100`B },	keyEncipherment
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 3 = Saphir 2 16 756 1 83 4 = Rubin},	In an end entity certificate, these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	"ldap://ldap.swissdigicert.ch: cn=Swisscom …objectClass= cRLDistributionPoint, " http://www.swissdigicert.ch/download/sdcs-(saphir)rubin.crl " },	[uRI], IA5String
extKeyUsage {		
extnId	{ 2 5 29 37 },	
extnValue	{ 1 3 6 1 5 5 7 3 4 } },	E-mail protection
AuthorityInfoAccess{		SEQUENCE{
extnId	{ 1 3 6 1 5 5 7 1 1 },	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessMethod	{ 1 3 6 1 5 5 7 48 2 },	id-ad-caIssuers
accessLocation	"http://www.swissdigicert.ch/download "},	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	"http://ocsp.swissdigicert.ch/rubin (oder saphir)" }}},	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 5},	sha1WithRSAsignarure
parameters	NULL },	RFC 3279
signature	`..... `B }	2048 Bit, BIT STRING

7.1.7 Server certificates (Ruby and Emerald) CA 1 for authentication and encryption

X.509 field	Value, OIDs	Comments
version	2,	Version 3
serialNumber	Unique integer	[Integer]
signature {		
algorithm	{1 2 840 113549 1 1 5}	sha1WithRSAsignarure
parameters	NULL },	RFC 3279
issuer	CN=Swisscom Sapphire(Ruby)-CA 1, O=Swisscom, OU=Digital Certificate Services, C=CH	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UCT, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ " },	UCT, ETSI TS 102 280
subject	{"CN=Given name Family name or Company, Organisation and E=name@provider.ch, C=Country, -- optional O= ,OU= , , SN=Date of birth,	directoryName, UTF8String, ETSI TS 102 280

X.509 field	Value, OIDs	Comments
	L=Place of birth "},	
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	RFC 3279
subjectPublicKey	'.....'B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subjectPublic-Key-BitString of "Q-CA 1"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subjectPublicKey-BitString of this subject/end entity"
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000011`B },	digitalSignature, nonRepudiation
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 3 = Saphir 2 16 756 1 83 4 = Rubin},	In an end entity certificate, these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	"ldap://ldap.swissdigicert.ch cn=Swisscom …..?objectClass= cRLDistributionPoint, " http://www.swissdigicert.ch/download/sdcs-(saphir)rubin.crl " },	[uRI], IA5String
extKeyUsage {		
extnId	{ 2 5 29 37 },	
extnValue	{1 3 6 1 5 5 7 3 1}, {1 3 6 1 5 5 7 3 2}},	serverAuth, clientAuth
AuthorityInfoAccess{		SEQUENCE{
extnId	{ 1 3 6 1 5 5 7 1 1 },	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessMethod	{ 1 3 6 1 5 5 7 48 2 },	id-ad-caIssuers
accessLocation	"http://www.swissdigicert.ch/policies"},	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	"http://ocsp.swissdigicert.ch/rubin (oder saphir)" }}},	[uRI], IA5String

X.509 field	Value, OIDs	Comments
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 5},	sha1WithRSAsignarure
parameters	NULL },	RFC 3279
signature	`...... `B }	2048 Bit, BIT STRING

7.2 CRL profile

The certificate revocation lists (CRL) are signed by the respective CAs using their own private keys.

All certificates issued by a CA and revoked during their period of validity appear in the CRL of the respective certification authority. The CRLs of Swisscom Digital Certificate Services are constructed according to the CRL v2 format.

Each CRL contains entries with the following information:

- Serial number of the revoked certificate
- Date of revocation
- Reason for revocation (optional)

CRLs are issued periodically at 24-hour intervals[2], and are valid for 7 days.

The LDAP tree node is:

dc = ch

dc = swissdigicert

cn = [CA-Name]

Attribute: certificateRevocationList

7.3 OCSP profile CA 1

The authority that signs reply to OCSP requests has the following certificate definition:

Attributes	Value, OIDs	Comments
ocspDirCertificate Certificate ::={		
tbsCertificate {		
version	2,	Version 3
serialNumber	10....	[Integer]
signature {		
algorithm	{1 2 840 113549 1 1 5}	sha1WithRSAsignarure
parameters	NULL },	
issuer	{ "CN=Swisscom Root CA 1, O=Swisscom, OU=Digital Certificate Services, C=CH" },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UCT, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ " },	UCT, ETSI TS 102 280
subject	{ "CN=Swisscom OCSP-DIR 1, O=Swisscom, OU=Digital Certificate Services, C=CH" },	directoryName, UTF8String
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption

[2] CRLs are also published each time a certificate is revoked.

Attributes	Value, OIDs	Comments
parameters	NULL },	
subjectPublicKey	'........'B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subjectPublicKey-BitString of "Root CA 1"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subject-PublicKey-BitString of "OCSP-DIR 1"
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000100010`B },	nonRepudation, cRLSign
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 2 1 } },	In a CA certificate, these policy information terms limit the set of policies for certification paths which include this certificate.
basicConstraints {		
extnId	{ 2 5 29 19 },	
critical	TRUE,	BOOLEAN
extnValue	{ cA FALSE },	BOOLEAN
pathLenConstraint	0 },	INTEGER
extendedKeyUsage {		
extnId	{ 2 5 29 37 },	
critical	TRUE,	BOOLEAN
extnValue	{1 3 6 1 5 5 7 3 9 } },	ocspSigning
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	"http://www.swissdigicert.ch/download/sSwisscom Digital Certificate Services-OCSP.crl" },	[uRI], IA5String
AuthorityInfoAccess{		
extnId	{ 1 3 6 1 5 5 7 1 1 },	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessMethod	{ 1 3 6 1 5 5 7 48 2 },	id-ad-caIssuers
accessLocation	"http://www.swissdigicert.ch/download"},	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	"http://ocsp.swissdigicert.ch" }}},	[uRI], IA5String
qcStatements {		
extnId	{ 1 3 6 1 5 5 7 1 3 },	
extnValue	SEQUENCE OF {	OCTET STRING
QCStatement	SEQUENCE {	

Attributes	Value, OIDs	Comments
statementId	{ 0 4 0 1862 1 1 }}}}}}	qcs-QcCompliance
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 5},	sha1WithRSAsignarure
parameters	NULL },	
signature	`..... `B }	2048 Bit, BIT STRING

OCSP Requests are handled in accordance with RFC 2560. The following status information is signed and returned:

Certificate Status	Certificate Status Value	Comments
Revoked	Revoked	
Suspended	Revoked	(not possible for qualified certificates)
Active	Good	
Unknown		Unknown

7.4 TSA Profile

7.4.1 Profile for Level 1 Time Stamp CA 1

X.509 field	Value, OIDs	Comments
version	2,	Version 3
serialNumber	xxxxxxx	1 or an alternative whole number [integer]
signature {		
algorithm	{1 2 840 113549 1 1 5}	sha1WithRSAsignarure
parameters	NULL },	
issuer	{ "CN=Swisscom Root CA 1, O=Swisscom, OU=Digital Certificate Services, C=CH" },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UCT, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ " },	UCT, ETSI TS 102 280
subject	{ "CN=Swisscom TSA CA 1, O=Swisscom, OU=Digital Certificate Services, C=CH },	directoryName, UTF8String
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	
subjectPublicKey	'........'B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subjectPublic-Key-BitString of "Root CA 1"
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN

X.509 field	Value, OIDs	Comments
extnValue	`000110000`B },	keyCertSign, cRLSign
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 5 1 } },	In a CA certificate, these policy information terms limit the set of policies for certification paths which include this certificate.
issuerAltName {		
extnId	{ 2 5 29 18 },	
extnValue	{ "O=ZertES-Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA" } },	directoryName, UTF8String
basicConstraints {		
extnId	{ 2 5 29 19 },	
critical	TRUE,	BOOLEAN
extnValue	{ cA TRUE },	BOOLEAN
pathLenConstraint	0 },	INTEGER, no other CA
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	"ldap://ldap.swissdigicert.ch/CN=Swisscom TSA CA 1,dc=tsa,dc=swissdigicert,dc=ch?certificateRevocationList?, http://www.swissdigicert.ch/download/sSwisscom Digital Certificate Services-TSA.crl" },	[uRI], IA5String
AuthorityInfoAccess{		SEQUENCE{
extnId	{ 1 3 6 1 5 5 7 1 1 },	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessMethod	{ 1 3 6 1 5 5 7 48 2 },	id-ad-caIssuers
accessLocation	"http://www.swissdigicert.ch/download"},	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	"http://ocsp.swissdigicert.ch" }}},	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 5},	sha1WithRSAsignarure
parameters	NULL },	
signature	`.....  `B }	2048 Bit, BIT STRING

Profile for Time Stamp Services (Luna SP)

Attributes	Value, OIDs	Comments
tsaCertificate Certificate ::={		
tbsCertificate {		
version	2,	Version 3
serialNumber	10....	[Integer]
signature {		
algorithm	{1 2 840 113549 1 1 5}	sha1WithRSAsignarure
parameters	NULL },	RFC 3279

Attributes	Value, OIDs	Comments
issuer	{ "CN=Swisscom TSA CA 1, O=Swisscom, OU=Digital Certificate Services},	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UCT, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ " },	UCT, ETSI TS 102 280
subject	{ "CN=Swisscom TSA 1, O=Swisscom, OU=Digital Certificate Services, C=CH, E=time@swissdigicert.ch" },	directoryName, UTF8String
subjectPublicKeyInfo {		
algorithm {		
algorithm	{1 3 14 3 2 26 },	hashAlgorithmIdentifier
parameters	NULL },	RFC 3279
subjectPublicKey	'........'B },	160 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subjectPublicKey-BitString of "Root CA 1"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	*1), OCTET STRING, composed of the 160-bit SHA-1 hash of subject-PublicKey-BitString of "TSA 1"
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000010`B },	nonRepudation
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 5 1 } },	ETSI TS 101 861 V1.2.1
issuerAltName {		
extnId	{ 2 5 29 18 },	
extnValue	{ "O=ZertES-Certification Body: KPMG Klynveld Peat Marwick Goerdeler SA" } },	directoryName, UTF8String
basicConstraints {		
extnId	{ 2 5 29 19 },	
critical	TRUE,	BOOLEAN
extnValue	{ cA FALSE },	BOOLEAN
pathLenConstraint	0 },	INTEGER
extendedKeyUsage {		
extnId	{ 2 5 29 37 },	
critical	TRUE,	BOOLEAN
extnValue	{1 3 6 1 5 5 7 3 8 } },	timeStamping
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	"http://www.swissdigicert.ch/download/sSwisscom Digital Certificate Services-TSA.crl" },	[uRI], IA5String

Attributes	Value, OIDs	Comments
AuthorityInfoAccess{		
extnId	{ 1 3 6 1 5 5 7 1 1 },	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessMethod	{ 1 3 6 1 5 5 7 48 2 },	id-ad-caIssuers
accessLocation	"http://www.swissdigicert.ch/download"}}},	[uRI], IA5String
SubjectInfoAccess{		
extnId	{ 1 3 6 1 5 5 7 1 11 },	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessMethod	{ 1 3 6 1 5 5 7 48 3 },	id-ad-timeStamping
accessLocation	"http://tsa.swissdigicert.ch" }}}}}	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 5},	sha1WithRSAsignarure
parameters	NULL },	RFC 3279
signature	`...... `B }	2048 Bit, BIT STRING

8 Compliance check

Rules are set out in the respective CP.

9 General provisions

Rules are set out in the respective CP.

10 Identification and authentication

Rules are set out in the respective CP.