Zertifikatsrichtlinien (CP/CPS)

zur Ausstellung von Zertifikaten der Klasse

„Rubin“ (fortgeschritten LCP)

Version: 3.3

Datum: 27. Januar 2022

Swisscom (Schweiz) AG
Digital Certificate Services
Postfach
8021 Zürich

Änderungskontrolle

Version	Datum	Ausführende Stelle	Bemerkungen/Art der Änderung
2.0	01.01.2012	Markus Limacher	beinhaltend CA 1 (Ersetzend) und CA 2 (NEU)
2.0	10.01.2012	Governance Board	Freigabe durch Ausschuss
2.1	22.03.2012	Hans-Peter Waldegger	Anpassungen Feedback KPMG zu ETSI 102 042
2.1	02.04.2012	Governance Board	Freigabe durch den Ausschuss
2.2	21.07.2014	Kerstin Wagner	Review und Update
2.3	02.10.2014	Patrick Graber	Ergänzung Rubin CA 3
2.4	04.06.2015	Kerstin Wagner	Review und Update
2.5	21.07.2015	Kerstin Wagner	Korrekturen im Kapitel 9.7 Haftung; Löschen der Verweise auf „fortgeschritten“ und „gemäss ZertES“.
2.6	12.01.2017	Kerstin Wagner	Auslagerung der Angaben zur CA der 1. Generation (CA 1) in ein eigenständiges Dokument; Review und Update 2016
3.0	30.04.2017	Kerstin Wagner; Hans-Peter Waldegger	Erstellung einer CP/CPS nach den neuen ETSI-Standards
3.1	18.04.2018	Kerstin Wagner	Ergänzungen nach der Konformitätsprüfung
3.1	18.04.2018	Governance Board	Freigabe
3.2		Kerstin Wagner	Anpassung Algorithmen und Schlüssellängen (Kap. 6.1.5) und div. Präzisierungen aufgrund Audit-Findings.
3.2	19.11.2018	Governance Board	Freigabe
3.3	22.03.2021	H-P Waldegger, K. Wagner	Ergänzung DN für Geräte-Zertifikate (Kap. 3.1.3), neue CA Hierarchie, Referenzen auf die Zertifikatsklasse "Smaragd" entfernt; Aktualisierung CRL und OCSP-Service, Aktualisierung und Ergänzung der Regularien
3.3	27.01.2022	QTSP Board	Freigabe

Referenzierte Dokumente:

[ZertES]	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, SR 943.03), in der Fassung vom 1. Januar 2017
[VZertES]	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Verordnung über die elektronische Signatur, SR 943.032), in der Fassung vom 1. Januar 2017
[TAV]	Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (SR 943.032.1), in der Fassung vom 1. Januar 2017
[UIDG]	Bundesgesetz über die Unternehmens-Identifikationsnummer, UIDG
[RFC 3647]	IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework"
[RFC 5280]	IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
[RFC 6960]	IETF RFC 6960: "Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol - OCSP"
[ETSI TS 119 312]	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[ETSI EN 319 401]	General Policy Requirements for Trust Service Providers
[ETSI EN 319 411-1]	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI EN 319 411-2]	Policy and security requirements for TSPs; Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETSI EN 319 412-1]	Certificate Profiles: Overview and common data structures
[ETSI EN 319 421]	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[Addendum]	Addendum zum CP/CPS: Profile der Zertifikate, Sperrlisten (CRL) und Online Statusabfragen
[NB]	Nutzungsbestimmungen
[Sicherheitskonzept]	Sicherheitskonzept SDCS
[Rollenkonzept]	Rollenkonzept SDCS

swisscom

Inhaltsverzeichnis

1 Einleitung 8
1.1 Überblick 8
1.2 Identifikation des Dokuments 8
1.3 Beteiligte der PKI 9
1.3.1 Certificate Authorities (CA) 9
1.3.2 Registrierungsstellen – Registration Authorities (RA) 10
1.3.3 Zertifikatsinhaber (Subscriber) 10
1.3.4 Zertifikatprüfer (Relying Parties) 10
1.3.5 Weitere Teilnehmer 10
1.4 Nutzung der Zertifikate (Certificate Usage) 11
1.4.1 Zulässige Zertifikatnutzung 11
1.4.2 Untersagte Zertifikatnutzung 11
1.5 Verwaltung der CP/CPS 11
1.6 Schlüsselwörter und Begriffe 12
1.7 Abkürzungen 15
2 Veröffentlichungen und Verantwortung für den Verzeichnisdienst 16
2.1 Verzeichnisdienst 16
2.2 Veröffentlichung von Informationen 16
2.3 Aktualisierung der Informationen 16
2.4 Zugang zu den Informationsdiensten 16
3 Identifizierung und Authentifizierung 17
3.1 Namen 17
3.1.1 Für natürliche Personen obligatorische Namensfelder 17
3.1.2 Für juristische Personen obligatorische Namensfelder 18
3.1.3 Für Geräte obligatorische Namensfelder 18
3.1.4 Optionale Namenselemente 19
3.1.5 Test-Zertifikate 19
3.2 Identitätsüberprüfung bei Neuantrag 19
3.2.1 Antrag einer natürlichen Person zur Selbstnutzung 19
3.2.2 Antrag für eine natürliche Person durch eine andere natürliche Person 20
3.2.3 Antrag für eine natürliche Person durch eine juristische Person 20
3.2.4 Antrag für eine juristische Person durch natürliche Personen 21
3.2.5 Antrag für eine juristische Person durch eine andere juristische Person 21
3.2.6 Nicht überprüfte Informationen 22
3.2.7 Verfahren zur Überprüfung des Besitzes des privaten kryptografischen Schlüssels 22
3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung 22
3.3.1 Routinemässige Zertifikatserneuerung (re-key) 22
3.3.2 Zertifikaterneuerung (re-key) nach einer Ungültigerklärung 22
3.4 Identifizierung und Authentifizierung bei einer Ungültigerklärung 22
4 Betriebsanforderungen für den Zertifikats-Lebenszyklus 22
4.1 Zertifikatantrag 22
4.2 Bearbeitung von Zertifikatsanträgen 23
4.3 Zertifikatausstellung 23
4.4 Zertifikatakzeptanz 23
4.5 Verwendung des Schlüsselpaares und des Zertifikats 23
4.5.1 Nutzung des privaten kryptografischen Schlüssels und des Zertifikats durch den Zertifikatinhaber 23
4.5.2 Nutzung von öffentlichen kryptografischen Schlüsseln und Zertifikaten durch Zertifikatprüfer 23
4.6 Zertifikaterneuerung unter Verwendung des alten Schlüsselpaares (Certificate Renewal) 24

4.7 Zertifikaterneuerung unter Verwendung eines neuen Schlüsselpaares (Re-Key) 24
4.8 Änderung von Zertifikaten 24
4.9 Ungültigerklärung und Suspendierung von Zertifikaten 24
4.9.1 Keine Ungültigerklärung bei kurzer Gültigkeitsdauer 24
4.9.2 Gründe für eine Ungültigerklärung 24
4.9.3 Wer kann die Ungültigerklärung vornehmen 25
4.9.4 Ablauf einer Ungültigerklärung eines Zertifikats 25
4.9.5 Fristen 25
4.9.6 CRL 25
4.9.7 Suspendierung 26
4.10 Dienst zur Statusabfrage von Zertifikaten 26
4.11 Beendigung des Vertragsverhältnisses durch den Zertifikatinhaber 26
4.12 Schlüsselhinterlegung und -wiederherstellung 26
5 Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen 26
5.1 Infrastrukturelle Sicherheitsmassnahmen 26
5.1.1 Lage und Konstruktion 26
5.1.2 Zutrittskontrolle 26
5.1.3 Stromversorgung und Klimatisierung 26
5.1.4 Abwehr von Wasserschäden 26
5.1.5 Feuer 27
5.1.6 Datenträger 27
5.1.7 Abfallentsorgung 27
5.1.8 Externes Backup 27
5.2 Organisatorische Sicherheitsmassnahmen 27
5.2.1 Vertrauenswürdige Rollen 27
5.2.2 Anzahl erforderlicher Mitarbeiter pro Aufgabe 27
5.2.3 Identifizierung und Authentisierung der Rollen 28
5.2.4 Trennung von Aufgaben 28
5.3 Personelle Sicherheitsmassnahmen 28
5.3.1 Anforderungen an die Mitarbeiter 28
5.3.2 Sicherheitsüberprüfung der Mitarbeiter 28
5.3.3 Anforderungen an die Schulung 28
5.3.4 Sanktionen für unautorisierte Handlungen 28
5.3.5 Dokumente für die Mitarbeiter 28
5.4 Sicherheitsüberwachung 29
5.4.1 Überwachte Ereignisse 29
5.4.2 Schutz der Protokolldaten 29
5.5 Archivierung 29
5.5.1 Archivierte Daten 29
5.5.2 Aufbewahrungszeitraum für archivierte Daten 29
5.5.3 Schutz der Archive 29
5.6 Schlüsselwechsel 29
5.7 Kompromittierung und Wiederherstellung 30
5.7.1 Prozeduren bei Sicherheitsvorfällen und Kompromittierung 30
5.7.2 Wiederherstellung von IT-Systemen 30
5.7.3 Kompromittierung von privaten kryptografischen Schlüsseln einer CA 30
5.7.4 Betrieb nach einer Katastrophe 30
5.8 Einstellung des Betriebes 30
6 Technische Sicherheitsmassnahm 30
6.1 Schlüsselerzeugung und Installation 30
6.1.1 Schlüsselerzeugung 30
6.1.2 Übermittlung des privaten kryptografischen Schlüssels an den Zertifikatsinhaber 31

6.1.3 Auslieferung des öffentlichen kryptografischen CA-Schlüssels ... 31
6.1.4 Algorithmen und Schlüssellängen ... 31
6.1.5 Parameter der öffentlichen kryptografischen Schlüssel und Qualitätssicherung ... 31
6.1.6 Verwendungszweck der Schlüssel und Beschränkungen ... 31
6.2 Schutz des privaten kryptografischen Schlüssels ... 31
6.2.1 Standard der kryptografischen Module ... 31
6.2.2 Teilung des privaten kryptografischen Schlüssels ... 31
6.2.3 Hinterlegung privater kryptografischer Schlüssel ... 31
6.2.4 Backup der privaten kryptografischen Schlüssel ... 31
6.2.5 Archivierung der privaten kryptografischen Schlüssel ... 32
6.2.6 Erstellung und Speicherung privater Schlüssel ... 32
6.2.7 Aktivierung der privaten kryptografischen Schlüssel ... 32
6.2.8 Deaktivierung der privaten kryptografischen Schlüssel ... 32
6.2.9 Vernichtung der privaten kryptografischen Schlüssel ... 32
6.2.10 Güte des kryptografischen Moduls ... 32
6.3 Weitere Aspekte des Schlüsselmanagements ... 32
6.3.1 Archivierung öffentlicher kryptografischer Schlüssel ... 32
6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren ... 32
6.4 Aktivierungsdaten ... 33
6.4.1 Aktivierungsdaten für Schlüssel von natürlichen Personen ... 33
6.4.2 Aktivierungsdaten für Schlüssel von Organisationen ... 33
6.4.3 Aktivierungsdaten für CA Schlüssel ... 33
6.5 Sicherheitsmassnahmen für Devices ... 33
6.5.1 Spezifische Anforderungen an technische Sicherheitsmassnahmen ... 33
6.5.2 Güte /Qualität der Sicherheitsmassnahmen ... 33
6.6 Lebenszyklus der Sicherheitsmassnahmen ... 33
6.6.1 Softwareentwicklung ... 33
6.6.2 Sicherheitsmanagement ... 33
6.7 Sicherheitsmassnahmen für das Netzwerk ... 34
6.8 Zeitstempel ... 34
7 Profile für Zertifikate, Sperrlisten (CRL) und Online-Statusabfragen ... 34
8 Konformitätsprüfung (Compliance Audit) und andere Assessments ... 34
8.1 Konformität ... 34
8.2 Zertifizierung ... 34
8.3 Intervall und Umstände der Überprüfung ... 34
8.4 Überprüfte Bereiche ... 34
8.5 Mängelbeseitigung ... 35
9 Rahmenbestimmungen ... 35
9.1 Vergütung ... 35
9.2 Haftpflichtversicherung von Swisscom ... 35
9.3 Vertraulichkeit von Geschäftsinformationen ... 35
9.3.1 Vertraulich zu behandelnde Daten ... 35
9.3.2 Nicht vertraulich zu behandelnde Daten ... 35
9.3.3 Verantwortung für den Schutz vertraulicher Informationen ... 35
9.4 Schutz von Personendaten (Datenschutz) ... 35
9.4.1 Allgemein ... 35
9.4.2 Verantwortlicher Umgang mit Personendaten ... 35
9.4.3 Offenlegung gegenüber Gerichten und anderen Behörden ... 36
9.4.4 Andere Umstände einer Weitergabe von Daten an Dritte ... 36
9.5 Urheberrechte ... 36
9.6 Gewährleistung ... 36

9.6.1 Gewährleistung von Swisscom ... 36
9.6.2 Gewährleistungen anderer Beteiligter ... 36
9.7 Haftung ... 36
9.7.1 Haftung von Swisscom ... 36
9.7.2 Haftung anderer Beteiligter ... 37
9.8 Inkrafttreten und Aufhebung ... 37
9.8.1 Inkrafttreten ... 37
9.8.2 Aufhebung ... 37
9.8.3 Konsequenzen der Aufhebung ... 37
9.8.4 Individuelle Benachrichtigungen und Kommunikation mit Zertifikatsinhabern ... 37
9.8.5 Änderungen dieses Dokuments ... 37
9.9 Konfliktbeilegung ... 37
9.10 Anwendbares Recht und Gerichtsstand ... 37
9.11 Einhaltung des anwendbaren Rechts ... 38
9.12 Sprache ... 38

1 Einleitung

Swisscom (Schweiz) AG betreibt als Zertifizierungsdiensteanbieter (ZDA) einen Zertifizierungsdienst für die Ausstellung von fortgeschrittenen, geregelten und qualifizierten Zertifikaten zur Nutzung für fortgeschrittene und qualifizierte Signaturen und fortgeschrittene und geregelte Siegel sowie zur Ausstellung von qualifizierten Zeitstempeln.

Dieses Dokument (nachfolgend "CP/CPS") beschreibt die Certificate Policy (Zertifikatsrichtlinien, CP) und das Certification Practice Statement (Aussagen über die Zertifizierungspraktiken, CPS) der Swisscom (Schweiz) AG, zur Ausgabe von digitalen Zertifikaten der Klasse „Rubin“.

1.1 Überblick

Die Struktur dieser CP/CPS orientiert sich an den Vorgaben des [RFC 3647].

Diese CP/CPS richtet sich nach den folgenden Standards des Europäischen Instituts für Telekommunikationsnormen für einen Zertifizierungsdiensteanbieter:

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI);
  General Policy Requirements for Trust Service Providers; [ETSI EN 319 401]
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI);
  Policy and security requirements for Trust Service Providers issuing certificates;
  Part 1: General requirements; [ETSI EN 319 411-1]

Um die internationale Zusammenarbeit mit anderen ZDA zu ermöglichen, kann diese CP/CPS in andere Sprachen übersetzt werden; massgeblich ist in jedem Fall die deutsche Version in der jeweils aktuellen Fassung.

1.2 Identifikation des Dokuments

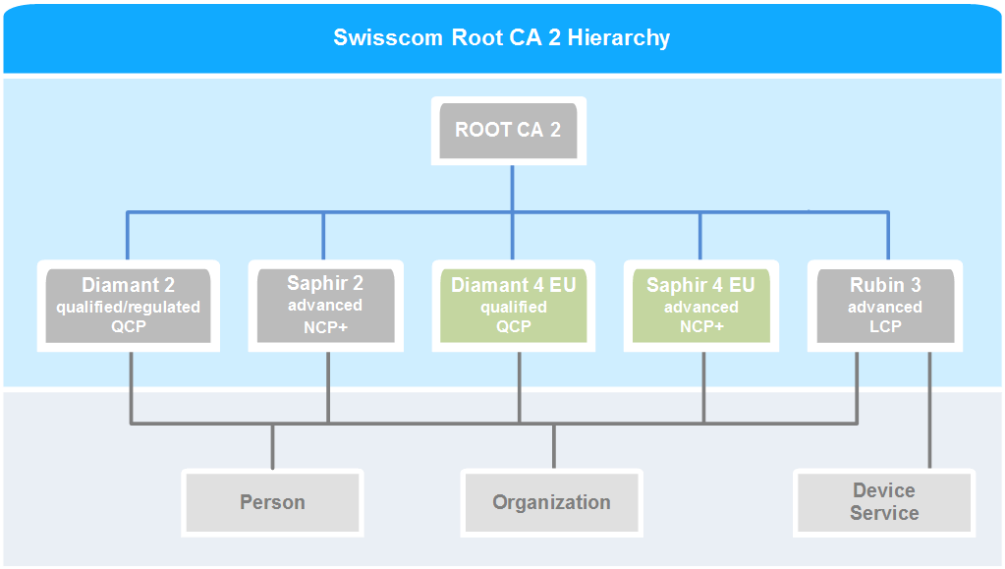
Titel:	Swisscom Digital Certificate Services – Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten der Klasse „Rubin“ (fortgeschritten LCP)“
Version:	3.3
Object Identifier:	2.16.756.1.83.22.0 - Rubin CA 3 2.16.756.1.83.30.4.4 - Rubin CA 4

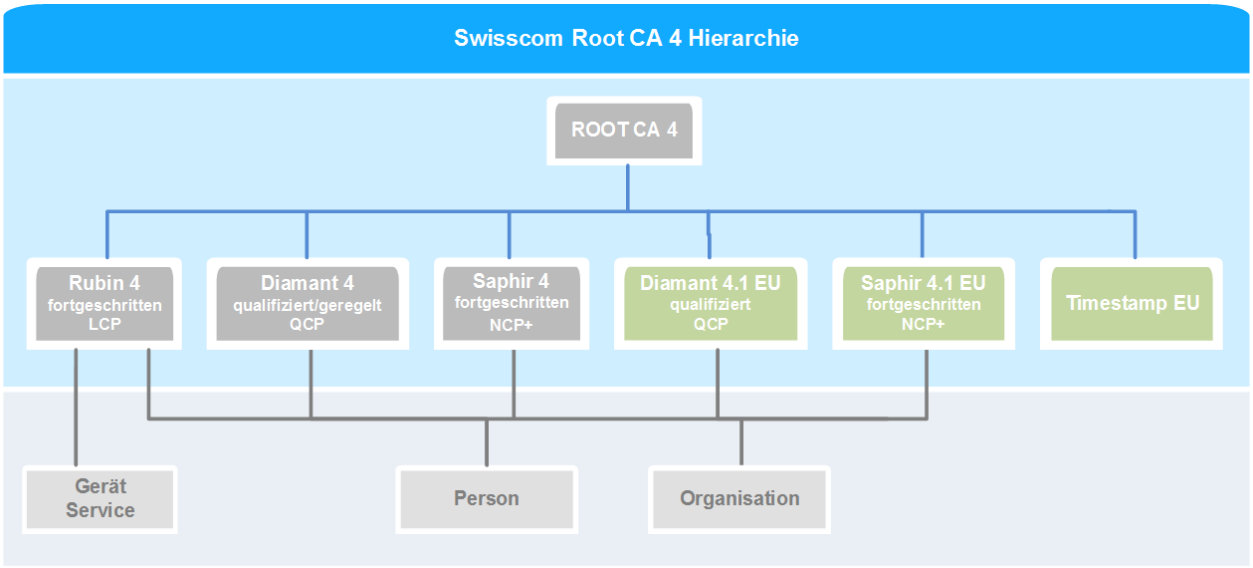
Die OID der Swisscom Digital Certificate Services basiert auf der vom schweizerischen Bundesamt für Kommunikation (BAKOM) zugeteilten RDN.

1.3 Beteiligte der PKI

1.3.1 Certificate Authorities (CA)

Die Public Key Infrastructure (PKI) der Swisscom ist hierarchisch aufgebaut:





Der Betrieb der hier dargestellten PKI erfolgt ausschliesslich durch Swisscom (Schweiz) AG, alle Systeme stehen in der Schweiz.

Verantwortlich für die mit dem Zusatz "EU" bezeichneten CAs ist Swisscom IT Services Finance S.E. mit Sitz in Wien. Diese CA erfüllen die sehr ähnlichen Anforderungen wie die an die gleichnamigen CA ohne den Zusatz "EU", richten sich jedoch nach der europäischen und österreichischen Gesetzgebung und sind Gegenstand einer eigenen Zertifikatsrichtlinie.

Root-CA

Die Swisscom Root CA ist an keinem Netzwerk angeschlossen und wird nur dann gestartet, wenn sie benötigt wird. Die Root-CA stellt ausschliesslich Zertifikate für unmittelbar nachgelagerte Certificate Authorities (CA) der Swisscom aus.

Unterhalb der Root-CA werden folgende CAs der Swisscom betrieben:

Diamant CA (gesetzlich geregelt)

Zur Ausgabe von Zertifikaten der Klasse „Diamant“ für natürliche Personen und UID-Einheiten. Entspricht den Definitionen für qualifizierte Zertifikate für qualifizierte elektronische Signaturen durch natürliche Personen von Art. 8 [ZertES] und für geregelte Zertifikate für geregelte elektronische Siegel für UID-Einheiten von Art. 7 [ZertES] sowie [ETSI EN 319 411-2] und verwendet ein sicheres kryptografisches Gerät (SCD).

Saphir CA (fortgeschritten – NCP+)

Zur Ausgabe von Zertifikaten der Klasse „Saphir“ für natürliche Personen und UID-Einheiten. Entspricht der Definition für ein fortgeschrittenes elektronisches Zertifikat zur Erstellung von fortgeschrittenen elektronischen Signaturen durch natürliche Personen und von fortgeschrittenen elektronischen Siegeln für UID-Einheiten und verwendet ein sicheres kryptografisches Gerät (SCD) gemäss [ETSI EN 319 411-1].

Rubin CA (fortgeschritten – LCP)

Zur Ausgabe von Zertifikaten der Klasse „Rubin“ für natürliche Personen und Organisationen (wie juristische Personen und Behörden). Entspricht den Definitionen für elektronische Zertifikate der Kategorie "Lightweight Certificate Policy" (LCP) gemäss [ETSI EN 319 411-1].

Time-Stamping-CA

Zur Ausgabe von Zeitstempel-Signaturen. Entspricht der Definition für qualifizierte elektronische Zeitstempel von Art. 2 Bst. j [ZertES] sowie [ETSI EN 319 411-2].

1.3.2 Registrierungsstellen – Registration Authorities (RA)

Die Registrierungsstellen identifizieren und authentifizieren Antragsteller, erfassen und prüfen die Anträge für verschiedene Zertifizierungsdienstleistungen, archivieren die Antragsdokumentation (geprüfte Dokumente, Vollmachten, etc.) und leiten die Daten an die Zertifizierungsstelle weiter. Swisscom kann die Aufgabe der Registrierung an Dritte (nachfolgend "RA-Partner") delegieren. RA-Partner werden mittels Vertrag verpflichtet, insbesondere die in diesem Dokument definierten Prozesse für die Registrierung, Zertifikatsausgabe, Revokation und Archivierung einzuhalten.

1.3.3 Zertifikatsinhaber (Subscriber)

Zertifikatsinhaber sind natürliche Personen oder Organisationen, die über den im Zertifikat definierten Namen eindeutig identifiziert werden können. Der Zertifikatsinhaber ist die Person bzw. die Organisation, die den privaten Schlüssel ihres Zertifikats besitzt und basierend auf diesem Zertifikat eine elektronische Signatur erstellt oder Daten verschlüsselt.

Swisscom kann Zertifikate für sich selbst ausstellen und als Zertifikatsinhaber auftreten. Für Swisscom gelten die gleichen Anforderungen wie für alle anderen Zertifikatsinhaber.

1.3.4 Zertifikatprüfer (Relying Parties)

Relying Parties sind natürliche Personen oder Organisationen, die die Zertifikate dieser PKI nutzen (z.B. Prüfung der Gültigkeit einer Signatur) und Zugang zu den Zertifizierungsdienstleistungen der Swisscom haben.

1.3.5 Weitere Teilnehmer

Weitere Teilnehmer können natürliche Personen oder Organisationen sein, die in den Zertifizierungs- oder Registrierungsprozess als Dienstleister eingebunden sind.

1.4 Nutzung der Zertifikate (Certificate Usage)

1.4.1 Zulässige Zertifikatnutzung

Die Zertifikate dürfen nur für die Anwendungen benutzt werden, die in Übereinstimmung mit der im Zertifikat angegebenen Nutzung (keyUsage) stehen.

Die im Rahmen dieser CP/CPS ausgestellten Zertifikate "Rubin" können zum Erstellen von digitalen Signaturen, zur Datenverschlüsselung, Clientauthentifizierung und für sicheres E-Mail verwendet werden

Die Schlüssel der Root-CA werden ausschliesslich zum Signieren der Zertifikate und Sperrlisten der Issuing CAs verwendet.

Die privaten Schlüssel der Issuing CA werden zum Signieren der zugehörigen Enduser-Zertifikate und OCSP-Signer Zertifikate benutzt.

1.4.2 Untersagte Zertifikatnutzung

Nutzungsarten, die nicht der im Zertifikat hinterlegten Nutzung (keyUsage) entsprechen, sind unzulässig. Swisscom haftet nicht für Schäden, die bei einer über diese Beschränkungen hinausgehenden Verwendung der Dienste entstanden sind.

1.5 Verwaltung der CP/CPS

Herausgeberin dieses Dokuments ist:

Swisscom (Schweiz) AG
Digital Certificate Services
Postfach
CH-8021 Zürich

Änderungen dieser CP/CPS werden durch das QTSP Board der Swisscom Digital Certificate Services genehmigt.

1.6 Schlüsselwörter und Begriffe

Begriff	Erklärung
Akkreditierungsstelle	Ein Bereich des Staatssekretariats für Wirtschaft (SECO), der Aufsichtsaufgaben in der Schweiz wahrnimmt, u.a. die Akkreditierung von → Anerkennungsstellen.
Anerkennungsstelle	Stelle, die nach der Bundesgesetzgebung für die Anerkennung und die Überwachung der Anbieterinnen von Zertifizierungsdiensten akkreditiert ist. Die Anerkennungsstelle wird in der Schweiz von Schweizerischen → Akkreditierungsstelle akkreditiert.
Base64	Verfahren zur Kodierung von 8-Bit-Binärdaten (z. B. Programme, ZIP-Dateien oder Bilder) in eine Zeichenfolge, die nur aus ASCII-Zeichen besteht.
Benutzer*in des Zertifikats (Relying Party)	Person oder Prozess, die oder der sich bei der Verwendung dieses Zertifikats auf die Angaben im Zertifikat verlässt.
Certifcation Practice Statement (CPS)	Angaben zu den Regeln und Richtlinien, die von vom ZDA für die Ausstellung von Zertifikaten effektiv umgesetzt werden. Die CPS definiert die Ausrüstungen, die Methoden und die Verfahren, die von ZDA in Übereinstimmung mit den von ihr gewählten Zertifikatsrichtlinien verwendet werden.
Certificate Authority (CA), Issuing CA	Instanz, die digitale Zertifikate ausstellt; in diesem Dokument wird damit das Device bezeichnet, das Zertifikate ausstellt und signiert; es ist das zentrale Element einer PKI Infrastruktur
Certificate Policy (CP)	Gesamtheit von Regeln, welche die Anwendbarkeit eines Zertifikats für einen bestimmten Personenkreis und/oder eine Klasse spezieller Anwendungen mit gemeinsamen Sicherheitsanforderungen vorschreiben.
CSR (Certificate Signing Request)	Digitaler Antrag, mittels einer digitalen Signatur aus einem öffentlichen kryptografischen Schlüssel ein digitales Zertifikat zu erstellen.
Digitales Zertifikat	elektronische Bescheinigung, die einen privaten kryptografischen Schlüssel (private key) mit dem Namen einer Person, einer Organisation oder eines Systems verknüpft.
Elektronische Signatur	Technisches Verfahren zur Überprüfung der Integrität eines Dokuments, einer elektronischen Nachricht oder der Identität des Absenders.
Elektronische Signaturerstellungseinheit, elektronische Siegelerstellungseinheit	Für die Implementierung des privaten kryptografischen Schlüssels konfigurierte Software/Firmware oder Hardware, den die Inhaberin oder der Inhaber des Zertifikats zur Erstellung einer elektronischen Signatur oder Siegels verwendet, z.B. eine SmartCard oder ein HSM.
Fortgeschrittenes Siegel	Das fortgeschrittene elektronische Siegel ist eine fortgeschrittene elektronische Signatur, die auf einem auf eine → UID-Einheit ausgestellten fortgeschrittenen Zertifikat beruht.
Fortgeschrittene Signatur	Die fortgeschrittene elektronische Signatur ist eine elektronische Signatur, die folgende Anforderungen erfüllt: 1. sie ist ausschliesslich der Inhaberin oder dem Inhaber zugeordnet, 2. sie ermöglicht die Identifizierung der Inhaberin oder des Inhabers, 3. sie wird mit Mitteln erzeugt, welche die Inhaberin oder der Inhaber unter ihrer oder seiner alleinigen Kontrolle halten kann, 4. sie ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann; (Art. 2 Bst. b [ZertES])
Generierung der Zertifikate	Dienst des ZDA; Erzeugung eines digitalen Zertifikats auf der Grundlage des Namens der Antragstellerin oder des Antragstellers eines Zertifikats und ihrer/seiner allfälligeren Attribute, die bei der Registrierung überprüft werden.

Begriff	Erklärung
Geregeltes elektronisches Siegel	Das geregelte elektronische Siegel ist eine fortgeschrittene elektronische Signatur, die unter Verwendung einer sicheren Siegelerstellungseinheit erstellt wurde und auf einem auf eine → UID-Einheit ausgestellten geregelten Zertifikat beruht (Art. 2 Bst. d [ZertES])
Hash	Die Hashfunktion ist eine kryptografische Prüfsumme für einen Text, um deren Integrität sicher zu stellen. Das Verfahren dient der Reduzierung des Rechenaufwandes bei der Verschlüsselung von Daten im Public-Key-Verfahren. Auf die Nachricht, die eine variable Länge hat, wird eine Hashfunktion angewendet, die eine Prüfsumme fester Länge erzeugt, den Hashwert. Damit lässt sich die Integrität einer Nachricht zweifelsfrei feststellen.
HSM (Hardware Security Module)	Device für die effiziente und sichere Ausführung kryptographischer Operationen oder Applikationen. HSMs bieten umfangreiche Funktionen zum sicheren Management des Gerätes und der privaten kryptografischen Schlüssel. In der Regel werden HSM zertifiziert, nach Sicherheitsstandards wie z. B. FIPS 140-2 oder Common Criteria (CC).
Inhaber/-in des Zertifikats (Subscriber)	Natürliche Person oder UID-Einheit, die Inhaberin des privaten kryptografischen Schlüssels ist, der dem im Zertifikat aufgeführten öffentlichen kryptografischen Schlüssel zugeordnet ist.
Liste der für ungültig erklärten Zertifikate (CRL)	von der CA signierte Liste, die die Seriennummern aller Zertifikate enthält, welche vor Ablauf ihrer Gültigkeit für ungültig erklärt wurden.
PKCS#10	Certification Request Standard aus der Familie der "Public Key Cryptography Standards".
Qualifizierte elektronische Signatur	Die „qualifizierte elektronische Signatur“ ist eine fortgeschrittene elektronische Signatur einer natürlichen Person, die von einer sicheren elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht (Art. 2 Bst. e [ZertES])
Sichere elektronische Signatur- oder Siegelerstellungseinheit	Signaturerstellungseinheit, die die Anforderungen von Artikel 6 [ZertES] erfüllt.
Qualifiziertes Zertifikat	Digitales Zertifikat, das die Anforderungen von Artikel 8 [ZertES] erfüllt.
RDN-Namen, Relative Distinguished Name	Namen der Verzeichniseinträge, deren Eindeutigkeit sich auf einen bestimmten Eintrag bezieht und die Bestandteile eines Verzeichnisnamens (Distinguished Name) sind.
Registrierung	Dienst der Registrierungsstelle, der darin besteht, die Identität und wenn nötig die Attribute jeder Antragstellerin und jedes Antragstellers eines Zertifikats zu überprüfen, bevor ihr/sein Zertifikat erzeugt oder die Aktivierungsdaten (oder das Passwort) zur Aktivierung der Nutzung des privaten kryptografischen Schlüssels zugewiesen werden.
Schlüsselpaar	privater kryptografischer Schlüssel und dazugehörender öffentlicher kryptografischer Schlüssel, die mathematisch durch einen asymmetrischen Signaturalgorithmus miteinander verknüpft sind.
Sicherheitspolitik (SP)	Gesamtheit von Regeln und Richtlinien, die auf Grund einer Risikoanalyse zur Reduzierung der Wahrscheinlichkeit von möglichen Zwischenfällen (vorbeugende Massnahmen) und zur Behebung der Auswirkungen solcher Zwischenfälle (Korrekturmassnahmen) ausgearbeitet wurden, um die für den ZDA als schützenswert identifizierten Ressourcen zu schützen. Mit der Sicherheitsstrategie und -politik kann die gesamthaft zu erreichende Sicherheitsstufe für ein Informationssystem und besonders für jedes Element der Sicherheitsarchitektur eindeutig definiert werden.
Öffentlicher kryptografischer Schlüssel (public key)	Daten wie Codes oder öffentliche kryptografische Schlüssel, die zur Überprüfung einer elektronischen Signatur oder Siegels oder zum Entschlüsseln verwendet werden.

Begriff	Erklärung
Privater kryptografischer Schlüssel (private key)	Einmalige Daten wie Codes oder private kryptografische Schlüssel, die von der Inhaberin oder vom Inhaber zur Erstellung einer elektronischen Signatur oder Siegels oder zum Verschlüsseln verwendet werden.
Time-stamping	Dienst des ZDA, der eine mit dem Datum, der Uhrzeit und einer qualifizierten Signatur versehene Bescheinigung abgibt, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt existiert haben.
Time-stamping Authority (TSA)	Instanz, die Zeitstempel-Objekte erstellt.
Time-stamping Policy (TP)	Spezifikation genereller Prozesse, die vom Zeitstempeldienst während des Erstellens von signierten Zeitstempeln verwendet werden.
Time-stamping token	Datenobjekt, welches die Darstellung einer Tatsache mit einem bestimmten Zeitpunkt verknüpft und so den Beweis liefert, dass die Tatsache vor dem Zeitpunkt existiert hat.
Time-stamping Unit	Die IT Infrastruktur, mit der Zeitstempel-Objekte erstellt werden können. Auf dieser Infrastruktur existiert nur ein privater kryptografischer Schlüssel zur Ausstellung von Zeitstempel-Objekten.
Trust Center	Speziell geschützter Raum, in dem die Infrastruktur des ZDA betrieben wird.
TSA Practice Statement (TPS)	Angaben zu den Regeln und Richtlinien, die von der Zeitstempeldienststelle für die Ausstellung von Zeitstempel-Objekten effektiv umgesetzt werden. Die TPS definiert die Ausrüstungen, die Methoden und die Verfahren, die vom Zeitstempel-Anbieter zur Ausgabe und Verwaltung von Zeitstempel-Objekten angewendet werden.
UID-Einheit	UID-Einheit nach Artikel 3 Absatz 1 Buchstabe c des Bundesgesetzes vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer [UIDG]. Hauptsächlich: - juristische Personen - Personengesamtheiten ohne Rechtsfähigkeit (z.B. einfache Gesellschaft) - Einzelfirmen - gewisse Verwaltungseinheiten von Bund, Kantonen und Gemeinden
Ungültigerklärung des Zertifikats	Dienst des ZDA, der die Gültigkeit eines Zertifikats vor dessen Ablauf aufhebt.
UTC, coordinated Universal Time	Universale Zeitskala auf Sekunden basierend. UTC ist definiert in der ITU-R Empfehlung TF.460-
Verteilung der Zertifikate	Dienst des ZDA, der darin besteht, das Zertifikat nach seiner Generierung der Inhaberin oder dem Inhaber und - bei Einwilligung der Inhaberin oder des Inhabers - den Benutzerinnen und Benutzern des Zertifikats zur Verfügung zu stellen.
Verwaltung des Zertifikatstatus	Dienst des ZDA, anhand dessen die Benutzerinnen und Benutzer eines Zertifikats überprüfen können, ob dieses für ungültig erklärt worden ist.
Zeitstempel-Dienst Benutzer (Subscriber)	Natürliche Person, die eigene oder Daten einer juristischen Person oder Organisation durch einen Zeitstempel-Dienst zeitstempelt.
Zertifizierungsdiensteanbieter (ZDA)	Eine Organisation, die digitale Zertifikate ausstellt und/oder andere Signatur- und Zertifizierungsdienste erbringt.
Zeitstempel-Objekt Empfänger (Relying Party)	Empfänger eines Zeitstempel-Objektes, der diesem Zeitstempel-Objekt vertraut

1.7 Abkürzungen

AIS	All-in Signing Service
CA	Certification Authority
CSIRT	Computer Security Incident Response Team
CN	Common Name, als Teil des DN
CP/CPS	Zertifikatsrichtlinien und Aussagen zu den Zertifizierungspraktiken
CRL	Certificate Revocation List
DN	Distinguished Name gemäss RFC 3739
eIDAS-VO	Verordnung Nr. 910/2014 des europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
ISO	Information Security Officer, IT Sicherheitsverantwortlicher
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol, Verzeichnisdienst
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol, Dienst zur Online Validierung von Zertifikaten
OID	Object Identifier
PED	PIN Entry Device
PIN	Personal Identification Number
QCP	Qualified Certificate Policy
RA	Registration Authority, Registrierungsstelle
Re-key	Zertifikaterneuerung basierend auf einem neuen Schlüsselpaar
SCD	Secure electronic Signature/Seal Creation Device, sichere elektronische Signaturerstellungseinheit gemäss ISO/IEC 15408
SSL	Secure Socket Layer, Sicherheitsprotokoll
TAV	Technische und administrative Vorschriften über elektronische Signaturen
TSA	Time-stamping Authority
UID	Unternehmens-Identifikationsnummer
UIDG	Bundesgesetz über die Unternehmens-Identifikationsnummer
ZDA	Zertifizierungsdiensteanbieter
VZertES	Verordnung über elektronische Signaturen
ZertES	Bundesgesetz über elektronische Signaturen

2 Veröffentlichungen und Verantwortung für den Verzeichnisdienst

2.1 Verzeichnisdienst

Swisscom stellt ihre CA-Zertifikate, Sperrlisten (CRL) der Root CAs, CP/CPS-Dokumente und Nutzungsbestimmungen im Web zur Verfügung.

Das Repository der Zertifizierungsdienste von Swisscom befindet sich auf:
https://trustservices.swisscom.com/repository/

Die Online-Dienste zur Abfrage der in Kapitel 2.2 aufgelisteten Informationen sind rund um die Uhr mit einer Verfügbarkeit von 99.9% zugänglich.

2.2 Veröffentlichung von Informationen

Auf der Website von Swisscom werden die folgenden Informationen publiziert:

- CP/CPS Dokumente
- Nutzungsbestimmungen
- Zertifikate der Root-und Issuing CAs, sowie der TSS CA und TSUs
- Sperr- und Widerrufsinformationen
- Revokationsinformationen im Falle einer Kompromittierung einer Root CA

Anpassungen in diesen Dokumenten werden gemäss den Angaben in Kapitel 9.8.4 kommuniziert.

Andere Zertifikate (insbesondere Benutzerzertifikate) werden nicht öffentlich publiziert.

2.3 Aktualisierung der Informationen

Neu ausgestellte Sperr- und Widerrufsinformationen, Richtlinien und ggf. weitere Informationen werden unmittelbar zur Verfügung gestellt. Es gelten die folgenden Veröffentlichungsfrequenzen:

- Sperr- und Widerrufsinformationen der Root CAs: nach Bedarf, jedoch mindestens einmal im Jahr
- OCSP: direkt nach einer Änderung
- CP/CPS-Dokumente: nach Änderungen bzw. nach Freigabe des Dokuments
- Weitere Informationen: nach Bedarf

2.4 Zugang zu den Informationsdiensten

Die unter den Kapiteln 2.1 und 2.2 aufgeführten Informationen sind öffentlich zugänglich.

3 Identifizierung und Authentifizierung

3.1 Namen

Die Identität des Zertifikatsinhabers wird im Zertifikat durch einen eindeutigen Namen (Distinguished Name, nachfolgend DN) entsprechend der Normenserie X.500 beschrieben. Ein DN besteht aus verschiedenen obligatorischen und optionalen Namenselementen.

Wählbare Namenselemente dürfen weder beleidigend noch anzüglich sein und nicht gegen Rechte Dritter (v.a. Namensrecht) oder sonstige Rechtsnormen verstossen. Die Registrierungsstelle ist nicht verpflichtet, den DN auf Konformität mit Rechten Dritter zu überprüfen. Allein der Zertifikatinhaber ist für solche Überprüfungen verantwortlich. Falls Swisscom bzw. die Registrierungsstelle über eine Verletzung solcher Rechte informiert wird, kann das Zertifikat von Swisscom für ungültig erklärt werden.

3.1.1 Für natürliche Personen obligatorische Namensfelder

Der DN natürlicher Personen muss aus Land, Anzeigename und entweder Vor-/Nachname oder Pseudonym bestehen und kann mit optionalen Elementen gemäss 3.1.3 ergänzt werden.

Element	X.520 Attribut	Inhalt	Bedeutung
Land	countryName (C)	Zweistelliger ISO 3166 Ländercode	Land, in dem der Zertifikatsinhaber seinen Wohnsitz hat, das vorgelegte Identifikations-Dokument des Zertifikatsinhabers ausgestellt wurde oder das zur Identitätsprüfung verwendete Register (z.B. Mitarbeiterverzeichnis) zugreifbar ist.
Anzeige-name	commonName (CN)	Informeller Name des Zertifikatsinhabers zur allgemeinen Darstellung.	Eine Darstellung des Namens, wie es der Zertifikatsinhaber oder der VDA zur benutzer- oder systemfreundlichen Darstellung für geeignet und verständlich hält.
Identität *entweder GN/SN*	givenName (G oder GN)	Formale(r) Vorname(n) des Zertifikatsinhabers	Exakte Wiedergabe des Inhalts des entsprechenden Feldes aus dem vorgelegten Identitätsdokument.
	surname (SN)	Formaler Familienname des Zertifikatsinhabers	Exakte Wiedergabe des Inhalts des entsprechenden Feldes aus dem vorgelegten Identitätsdokument.
oder	pseudonym	Abstrakte Zeichenfolge/Alias	Beliebige Zeichenfolge, welche den Zertifikatsinhaber im Kontext der PKI eindeutig Identifiziert. Die Identität des Inhabers muss nicht ohne Zusatzinformationen aus dem Zertifikat erkennbar sein.
Eindeutig-keit	serialNumber	Abstrakte Zeichenfolge, welche die Eindeutigkeit des DN sicherstellt.	Zeichenfolge gemäss einer der folgenden Definitionen: • Von Swisscom vergebene Seriennummer • Von einer Swisscom Registrierungsstelle vergebene Seriennummer mit eindeutigem Präfix • Zeichenfolge gemäss ETSI EN 319 412-2 "Natural person semantics identifier" • vor dem 1. März 2018 verwendete Formate Bei Verwendung eines Pseudonyms oder E-Mail-Adresse, welches die Eineindeutigkeit sicherstellt, kann die serialNumber weggelassen werden.

3.1.2 Für juristische Personen obligatorische Namensfelder

Der DN juristischer Personen muss aus Land, Anzeigename, der Firma (Namen) gemäss Eintrag im Firmenbuch (Handelsregister) und einer aus dem Unternehmenssteuer-Identifikationsnummer (UID) abgeleiteten Bezeichnung bestehen und kann mit optionalen Elementen gemäss 3.1.3 ergänzt werden.

Element	X.520 Attribut	Inhalt	Bedeutung
Land	countryName (C)	Zweistelliger ISO 3166 Ländercode	Land, in dem der Zertifikatsinhaber seinen Wohnsitz hat oder das vorgelegte Identifikations-Dokument des Zertifikatsinhabers ausgestellt wurde.
Anzeige-name	commonName (CN)	Informeller Name des Zertifikatsinhabers zur allgemeinen Darstellung.	Eine Darstellung des Namens, wie es der Zertifikatsinhaber oder die VDA zur benutzer- oder systemfreundlichen Darstellung für geeignet und verständlich hält.
Identität	organization Name (O)	Formale Firma (Name des Unternehmers, unter dem er seine Geschäfte betreibt) des Zertifikatsinhabers	Exakte Wiedergabe des Inhalts des entsprechenden Feldes aus dem vorgelegten Identitätsdokument.
Eindeutigkeit	organization Identifier	Aus amtlicher Registernummer der Organisation abgeleitete Zeichenfolge	Zeichenfolge gemäss ETSI EN 319 412-3 "Legal person semantics identifier"

3.1.3 Für Geräte obligatorische Namensfelder

Um Anwendungsfälle zu ermöglichen, die die Identität von Zertifikatsinhabern indirekt über Geräte-Zertifikate nachweisen, kann ein DN auf ein Gerät ausgestellt werden. Die weiteren Anforderungen an diese Zertifikate (z.B. Identifikation) richten sich nach der Person, deren Identität durch den Besitz des Geräts bestätigt werden soll.

Der DN zur eindeutigen Identifikation von Geräten (Devices) muss aus Land, Anzeigename und einer die Eindeutigkeit des Geräts sicherstellende Bezeichnung bestehen und kann mit optionalen Elementen gemäss 3.1.3 ergänzt werden.

Element	X.520 Attribut	Inhalt	Bedeutung
Land	countryName (C)	Zweistelliger ISO 3166 Ländercode	Land, in dem die Anwendung betrieben wird, die das Gerät verwaltet
Anzeige-name	commonName (CN)	Informelle Bezeichnung des Geräts zur allgemeinen Darstellung.	Eine Darstellung des Namens, wie es die beantragende Anwendung zur benutzer- oder systemfreundlichen Darstellung für geeignet und verständlich hält.
Eindeutigkeit	serialNumber	Abstrakte Zeichenfolge, welche die Eindeutigkeit des DN sicherstellt.	Zeichenfolge, die sicherstellt, dass der resultierende DN immer auf ein definiertes von der beantragenden Anwendung verwaltetes Gerät verweist. Die Zeichenfolge muss mit einem eindeutigen, von der Swisscom Registrierungsstelle vorgegebenen Präfix beginnen. Bereits vergeben sind: MID - Mobile ID SAS – Signature Activation Service

3.1.4 Optionale Namenselemente

X.520 Attribut	Inhalt	Bedeutung
organization Name (O)	Identifizierende Organisation	Bei natürlichen Personen kann eine Organisationsbezeichnung hinzugefügt werden, welche die Eindeutigkeit des Namens sicherstellt. Weitergehende Interpretationen des Verhältnisses des Zertifikatsinhabers zur Organisation sind nicht zulässig.
organizational Unit (OU)	Teilbereich innerhalb der Organisation.	Bei Angabe einer Organisation (O=), können von der bezeichneten Organisation eine oder mehrere Organisationseinheiten definiert werden. Die Rolle und das Verhältnis des Zertifikatsinhabers zu den Organisationseinheiten ist nicht definiert.
stateOr ProvinceName (ST)	Kanton/Bundesland	Geografischer Teilbereich des Landes (C=), in dem der Zertifikatsinhaber seinen (Wohn-)Sitz hat oder das vorgelegte Identifikations-Dokument des Zertifikatsinhabers ausgestellt wurde.
localityName (L)	Ortschaft	Ortschaft, in dem der Zertifikatsinhaber seinen (Wohn-)Sitz hat oder das vorgelegte Identifikations-Dokument des Zertifikatsinhabers ausgestellt wurde.
emailAddress	Eine E-Mail-Adresse des Zertifikatsinhabers	Vom Zertifikatsinhabers angegebene und zum Zeitpunkt der Identifikation vom Zertifikatsinhaber verwaltete E-Mail-Adresse. Sofern innerhalb des Zertifikats weitere E-Mail Namenselemente aufgenommen werden (z.B. alternativer Inhabername), müssen diese beiden Inhalte exakt übereinstimmen.

3.1.5 Test-Zertifikate

Zertifikate zu Testzwecken sind ausnahmsweise zulässig, wenn deren Ausstellung für die Vorbereitung oder die Prüfung des ordentlichen produktiven Einsatzes notwendig sind. Die Anzahl der Test-Zertifikate ist tief zu halten. Die Test-Zertifikate müssen sowohl im Anzeigename (CN) wie auch in einer evtl. vorhandenen Organisationsbezeichnung eindeutig den Ausdruck "TEST" enthalten.

Pseudonyme sind für Test-Zertifikate nur zugelassen, wenn sie ein allgemein Nachvollziehbares Identitätsmerkmal (z.B. Mobilfunknummer, Ausweisnummer) enthalten.

3.2 Identitätsüberprüfung bei Neuantrag

Für die Identitätsprüfung des Antragstellers auf fortgeschrittene Zertifikate sind die nachfolgenden Verfahrensschritte einzuhalten.

3.2.1 Antrag einer natürlichen Person zur Selbstnutzung

Für die Identitätsprüfung des Antragstellers auf fortgeschrittene Zertifikate sind die nachfolgenden Verfahrensschritte einzuhalten:

1. Der Antragsteller muss anhand eines Lichtbildausweises identifiziert werden, auf welchem Name und Vorname maschinell (nicht handschriftlich) aufgebracht sind. Darunter fallen insbesondere
    a. Führerausweis
    b. Ausländerausweis
    c. SwissPass des Schweizerischen Verbands öffentlicher Verkehr
    d. Generalabonnement der Schweizerischen Bundesbahn oder analoges Abonnement ausländischer Transportunternehmen (z.B. BahnCard 100 der Deutschen Bahn)
    e. Mitarbeiter-/Personalausweis einer UID-Einheit, die in der Schweiz AHV-pflichtig ist

Ein Nachweis, dass die Identitätsprüfung bereits in einem für höherwertige Zertifikatsklassen gemäss Kap. 1.3.1 ausreichendem Umfang durchgeführt wurde, ist ebenfalls zulässig.

2. Sofern im vorgelegten Lichtbildausweis kein Geburtsdatum und Geburts- oder Heimatort aufgeführt sind, muss der Antragsteller dies durch weitere offizielle Dokumente belegen.
3. Die Registrierungsstelle führt eine optische Prüfung der vorgelegten Dokumente durch und validiert ihre Übereinstimmung mit den Angaben des Gesuchs. Geprüft werden Name, Vorname und alle im Zertifikat zu vermerkenden Attribute.
4. Die Registrierungsstelle führt die Identitätsprüfung anhand des vorgelegten Identitätsnachweises durch.
5. Die Registrierungsstelle überprüft das Vorhandensein und die Korrektheit entweder
    a. der Mobiltelefonnummer des Antragstellers oder
    b. einer E-Mail-Adresse des Antragsstellers

    und registriert das Medium als berechtigtes Authentisierungsmittel für spätere Anpassungen der Benutzerdaten oder Zertifikatsrevokation.

Nach Akzeptanz der Nutzungsbestimmungen wird der Antrag zur weiteren Ausführung gemäss Kapitel 4.3. an Swisscom weitergeleitet.

Der Zertifikatsantrag und die Identitätsnachweise werden 2 Jahre aufbewahrt.

Bei Anträgen auf Einschluss einer Organisationsbezeichnung (O=) im DN werden folgende zusätzliche Prüfungen durchgeführt:

1. Bestätigung des Einverständnisses der Organisation zur Verwendung der gewünschten Namenselemente im Zertifikat;
2. Nachweis der Firmen- oder Namensrechte der Organisation auf gewünschte Organisationsbezeichnung.

Verfügt die beantragende Person bereits über ein gültiges Zertifikat, kann die Beantragung weiterer Zertifikate der gleichen oder niedrigeren Güte (gemäss Kap. 1.3.1) für diese Person auch durch die Übersendung eines elektronisch signierten Antrags erfolgen.

3.2.2 Antrag für eine natürliche Person durch eine andere natürliche Person

Stellvertretung wird bei Anträgen für natürliche Personen nicht unterstützt.

3.2.3 Antrag für eine natürliche Person durch eine juristische Person

Bei Anträgen für eine natürliche Person, welche durch eine juristische Person eingereicht wird, sind die nachfolgenden Verfahrensschritte einzuhalten:

1. Die juristische Person (Antragssteller) muss folgende Vorbedingungen erfüllen:
    a. Der Antragsteller muss einen Vertrag mit Swisscom für den Bezug einer Dienstleistung haben, die (teilweise) auf Zertifikaten für natürliche Personen basiert.
    b. Der Antragsteller hat schriftlich bestätigt, ausschliesslich Anträge für natürliche Personen zu stellen, die der Antragssteller gemäss den Anforderungen im Kapitel 3.2.1 bereits in seiner Organisation identifiziert hat.
    c. Der Antragssteller hat einen Nachweis erbracht, die Firmen- oder Namensrechte der Organisation auf gewünschte Organisationsbezeichnung zu besitzen.
    d. Der Antragssteller stimmt der Aufnahme seiner Organisationsbezeichnung im Zertifikat zu
2. Der Antrag beinhaltet entweder folgende Angaben, der Antragssteller gewährt Swisscom Zugriff auf einem organisationsspezifischen Verzeichnis oder Swisscom verfügt selbst über einen Zugriff auf ein Register, das folgende Daten enthält:

a. Name und Vorname, und
b. Geburtsdatum, und
c. Geburts- oder Heimatort, und
d. Mobiltelefonnummer oder E-Mail-Adresse der natürlichen Person

3. Der Antrag beinhaltet die Verwendung der Organisationsbezeichnung des Antragstellers.
4. Die Registrierungsstelle prüft die Vollständigkeit der vorgelegten Dokumente. Die Antragstellende Organisation muss entweder in der Organisationsbezeichnung des DN des Zertifikatsinhabers und/oder im alternativen Inhabername als E-Mail-Adresse des Zertifikatsinhabers innerhalb der antragstellenden Organisation vorkommen.
5. Die Registrierungsstelle überprüft das Vorhandensein und die Korrektheit entweder
   a. der Mobiltelefonnummer des Zertifikatsinhabers oder
   b. einer E-Mail-Adresse des Zertifikatsinhabers

   und registriert das Medium als berechtigtes Authentisierungsmittel für spätere Anpassungen der Benutzerdaten oder Zertifikatsrevokation.

Nach Akzeptanz der Nutzungsbestimmungen wird der Antrag zur weiteren Ausführung gemäss Kapitel 4.3. an Swisscom weitergeleitet.

Der Zertifikatsantrag und die Identitätsnachweise werden 2 Jahre aufbewahrt.

3.2.4 Antrag für eine juristische Person durch natürliche Personen

Für die Überprüfung von Anträgen juristischer Personen für fortgeschrittene Zertifikate sind folgende Verfahrensschritte anwendbar:

1. Der Vertreter des Antragsstellers muss eine natürliche Person sein (auch mehrere natürliche Personen können die Vertretung gemeinsam ausüben, insbesondere bei Kollektivzeichnungsberechtigung).
2. Der Vertreter des Antragstellers hat beizulegen.
   a. einen Auszug aus dem Handelsregister;
   b. einen unterschriebenen Zertifikatsantrag mit den gewünschten Zertifikatsangaben und einen Nachweis aller gewünschten Attribute;
      i. organizationName muss dem Namen gemäss Handelsregister entsprechen
      ii. stateOrProviceName muss dem Sitz gemäss Handelsregister entsprechen
      iii. localityName muss dem Firmensitz Sitz gemäss Handelsregister entsprechen
      iv. emailAddress: Bestätigung (Email, Fax, SMS, oder Brief) des Domänenkontakts gemäss whois.nic.ch
   c. Die Mobilnummer eines alleine berechtigen Vertreters des Antragsstellers (Kontakt) in der Zukünftigen Kommunikation mit Swisscom (insbesondere Revokation des Zertifikats).
3. Die Registrierungsstelle überprüft die vorgelegten Dokumente und validiert ihre Übereinstimmung mit den Angaben des Gesuchs.

Die Antragsteller bestätigen ihr Einverständnis zu dem oben beschriebenen Verfahren und die Akzeptanz der Swisscom Nutzungsbedingungen für die entsprechende Zertifikatsklasse

Der Zertifikatsantrag und die Identitäts- und Vertretungsnachweise werden 2 Jahre aufbewahrt.

3.2.5 Antrag für eine juristische Person durch eine andere juristische Person

Vertretung durch eine juristische Person wird nicht unterstützt.

3.2.6 Nicht überprüfte Informationen

Es werden alle Informationen überprüft, die im Zertifikat aufgenommen werden. Darüber hinaus werden keine weiteren Informationen überprüft.

3.2.7 Verfahren zur Überprüfung des Besitzes des privaten kryptografischen Schlüssels

Bei Schlüsselgenerierung durch den Antragsteller muss der Zertifikatsantrag einen Base64 codierten PKCS#10 CSR (Certificate Signing Request) beinhalten. Der Antrag muss mit dem privaten kryptografischen Schlüssel signiert werden, welches zum beantragten öffentlichen kryptografischen Schlüssel passt.

Bei Schlüsselgenerierung durch Swisscom werden die privaten kryptografischen Schlüssel innerhalb einer geschützten Umgebung gehalten. Anwendungen, die innerhalb der Swisscom laufen, brauchen deshalb keinen zusätzlichen Nachweis des Besitzes des privaten kryptografischen Schlüssels.

3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung

3.3.1 Routinemässige Zertifikatserneuerung (re-key)

Sofern keine noch nicht überprüften Attribute im neuen Zertifikat aufgenommen werden sollen, sind für eine Zertifikatserneuerung keine zusätzlichen Massnahmen zur Identifikation des Antragsstellers nötig. Voraussetzung für diese Art der Antragstellung ist, dass die Registrierungsstelle die Identität des Antragstellers innerhalb der letzten sieben Jahre nach Kapitel 3.2 festgestellt hat.

Für alle anderen Fälle ist wie für einen Neuantrag (Kapitel 3.2) zu verfahren.

3.3.2 Zertifikaterneuerung (re-key) nach einer Ungültigerklärung

Nach Ungültigerklärung eines Zertifikats erfolgt keine Zertifikaterneuerung. Es ist ein neues Zertifikat zu beantragen. Es gilt das Verfahren nach Kapitel 3.2.

3.4 Identifizierung und Authentifizierung bei einer Ungültigerklärung

Anträge auf Revokation werden durch die bei der Registrierung hinterlegten Authentisierungsmittel autorisiert.

Ungültigerklärung durch natürliche Personen:

- Persönliche Mobiltelefonnummer des Antragstellers bei persönlichen Zertifikaten.

Ungültigerklärung durch juristische Personen.

- Persönliche Mobiltelefonnummer einer der Vertreter des Antragstellers bei Zertifikaten juristischer Personen.

Sollte der Zertifikatsinhaber sein Identifikationsmittel verloren haben, kann er die Revokation auch durch Übersendung eines unterzeichneten Widerrufsantrags unter Angabe der Seriennummer des Zertifikates per Post einreichen. Zur Verifikation der Identität wird der Zertifikatsinhaber während der Geschäftszeit über die Firmenzentrale zurückgerufen.

4 Betriebsanforderungen für den Zertifikats-Lebenszyklus

4.1 Zertifikatantrag

Zertifikatsanträge können von natürlichen Personen oder Organisationen bei Registrierungsstellen der Swisscom (insbesondere bei RA-Partnern) gestellt werden. Es gilt das Verfahren nach Kapitel 3.2.

4.2 Bearbeitung von Zertifikatsanträgen

Die Registrierungsstelle führt die Identifikation und Authentifizierung eines Antragstellers nach den im Abschnitt 3.2 genannten Verfahren durch und teilt dem Antragsteller anschliessend mit, bis wann sein Antrag verifiziert werden kann. Nach erfolgreicher Verifikation durch die Registrierungsstelle wird der Zertifikatantrag innerhalb von maximal 10 Arbeitstagen durch Swisscom weiterbearbeitet:

4.3 Zertifikatausstellung

Nach erfolgreicher Verifikation des Zertifikatsantrags durch die Registrierungsstelle werden die Anträge elektronisch als signierte CSR zur Verarbeitung weitergeleitet. Nach erfolgreicher Prüfung der Einhaltung der erforderlichen Richtlinien stellt Swisscom der Registrierungsstelle das Zertifikat bereit.

- Bei Schlüsselgenerierung durch den Antragsteller wird das Zertifikat durch die Registrierungsstelle an den Zertifikatsinhaber verschickt oder zur Nutzung bereitgestellt.
- Bei Schlüsselgenerierung durch Swisscom werden die Aktivierungsdaten für die Nutzung des privaten kryptografischen Schlüssels entweder direkt an den Zertifikatsinhaber versandt oder die hinterlegten Zugriffsdaten (z.B. Mobiltelefonnummer) können direkt zur Freigabe des privaten kryptografischen Schlüssels eingesetzt werden.

4.4 Zertifikatakzeptanz

Durch Verwendung des Zertifikats bzw. durch Freigabe der Signaturerstellung bei Fernsignaturen bestätigt der Zertifikatsinhaber die Korrektheit der bei der Registrierungsstelle hinterlegten Daten und akzeptiert das mit der Signatur verknüpfte Zertifikat.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Nutzung des privaten kryptografischen Schlüssels und des Zertifikats durch den Zertifikatinhaber

Durch die Verwendung des Zertifikats versichert der Zertifikatinhaber allen Beteiligten im Sinn von Kapitel 1.3, dass:

- sämtliche Angaben und Erklärungen des Zertifikatinhabers in Bezug auf die im Zertifikat enthaltenen Informationen der Wahrheit entsprechen,
- die Signaturerstellungsdaten (z.B. PIN oder Passwort) für die Freigabe der Signatur- bzw. Siegelerstellung gemäss den Nutzungsbestimmungen der Swisscom behandelt werden,
- das Zertifikat ausschliesslich in Übereinstimmung mit dieser CP/CPS eingesetzt wird.

Der Zertifikatsinhaber, der die kryptografischen Schlüssel selbst generiert hat, versichert zudem, dass

- ein angemessenes Verständnis der Anwendung und des Einsatzes von Zertifikaten besteht,
- der private kryptografische Schlüssel geschützt aufbewahrt wird,
- keiner unbefugten Person Zugang zum privaten kryptografischen Schlüssel gewährt wird,
- er unverzüglich auf den weiteren Einsatz des privaten kryptografischen Schlüssels verzichtet, wenn die Angaben des Zertifikats nicht mehr stimmen oder der private Schlüssel abhandenkommt, gestohlen wurde oder sonst möglicherweise Dritten zur Kenntnis gelangt ist (Kompromittierung).

4.5.2 Nutzung von öffentlichen kryptografischen Schlüsseln und Zertifikaten durch Zertifikatprüfer

Jede Person, die als Relying Party im Sinn von Kapitel 1.3 den öffentlichen kryptografischen Schlüssel des Zertifikats gemäss dieser CP/CPS verwendet, muss

- ein grundlegendes Verständnis der Anwendung und des Einsatzes von Zertifikaten besitzen;

- geeignete Komponenten und Verfahren zur Prüfung der Angaben im Zertifikat einsetzen;
- die entsprechende OCSP-Antwort überprüfen, bevor sie sich auf die Angaben in einem Zertifikat verlässt.

4.6 Zertifikaterneuerung unter Verwendung des alten Schlüsselpaares (Certificate Renewal)

Swisscom kann in begründeten Ausnahmefällen ein neues Zertifikat basierend auf einem bereits verwendeten Schlüsselpaar (certificate renewal) ausstellen, sofern das erneuerte Zertifikat für den gleichen Zertifikatsinhaber vorgesehen ist. Zur Unterscheidung vom ursprünglichen Zertifikat muss das erneuerte Zertifikate eine unterschiedliche Seriennummer erhalten.

Die Identifikation des Zertifikatsinhabers muss den Anforderungen aus Kapitel 3.2.1 genügen.

4.7 Zertifikaterneuerung unter Verwendung eines neuen Schlüsselpaares (Re-Key)

Ein Zertifikatsinhaber kann bei einer Registrierungsstelle ohne Begründung einen Antrag auf Ausstellung eines neuen Zertifikats mit neuem Schlüsselpaar (re-key) stellen.

Swisscom wird nach positiver Authentifizierung des Zertifikatsinhabers gemäss Kapitel 3.2ein neues Zertifikat unter Verwendung der bereits überprüften Daten ausstellen, sofern der Zertifikatsinhaber noch die gleichen Authentisierungsmittel besitzt. Der Zertifikatinhaber hat zu bestätigen, dass die bei der Identifikation (siehe Kapitel 3.2) aufgenommenen Informationen weiterhin gültig sind.

Es kommen die zum Zeitpunkt der Zertifikatserneuerung gültige CP/CPS und Nutzungsbestimmungen zur Anwendung.

4.8 Änderung von Zertifikaten

Swisscom nimmt keine Änderungen von bereits ausgestellten Zertifikaten vor.

4.9 Ungültigerklärung und Suspendierung von Zertifikaten

4.9.1 Keine Ungültigerklärung bei kurzer Gültigkeitsdauer

Für Zertifikate, deren Gültigkeitsdauer weniger als 1 Stunde beträgt, wird keine Ungültigerklärung vorgenommen.

4.9.2 Gründe für eine Ungültigerklärung

Zertifikatsinhaber müssen ihre Zertifikate unverzüglich für ungültig erklären, wenn

- der private kryptografische Schlüssel oder sonstige Zugriffsdaten für die Verwendung des privaten kryptografischen Schlüssels verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht wurden oder werden können;
- das betroffene Zertifikat nicht mehr benötigt wird;
- die Gefahr einer missbräuchlichen Verwendung des Zertifikats besteht;
- die Angaben im Zertifikat nicht korrekt sind.

Zertifikate können von Swisscom für ungültig erklärt werden, wenn:

- der Zertifikatsinhaber (natürliche Person oder UID-Einheit) einen entsprechenden Antrag stellt oder
- Swisscom mindestens einer der folgenden Gründe bekannt wird:
  - Kenntnis vom Ableben des Zertifikatinhabers oder sonst von der Änderung im Zertifikat bescheinigter Umstände;

- der private kryptografische Schlüssel des Zertifikatinhabers oder derjenige von Swisscom für eine ausstellende CA verloren, gestohlen, offengelegt oder anderweitig kompromittiert bzw. missbraucht wurde;
- das Zertifikat aufgrund falscher Angaben erwirkt wurde;
- Swisscom ihre Tätigkeit ganz oder teilweise einstellt und ihre Verzeichnis- und Widerrufsdienste nicht von einem anderen ZDA übernommen werden;
- der Zertifikatinhaber diese CP/CPS nicht einhält;
- die zuständige Registrierungsstelle diese CP/CPS nicht einhält;
- der Zertifikatinhaber seiner Zahlungspflicht für die Gebühren auch nach mehrmaliger Aufforderung nicht nachkommt;
- einer der Gründe für Ungültigkeitserklärung durch den Zertifikatsinhaber vorliegt.

4.9.3 Wer kann die Ungültigerklärung vornehmen

Zertifikate können grundsätzlich nur von Swisscom für ungültig erklärt werden. Jeder Zertifikatinhaber kann von der Registrierungsstelle, die sein Zertifikat erstellt hat, unter Angabe von Gründen verlangen, dass diese ein für ihn ausgestelltes Zertifikat ungültig erklärt.

4.9.4 Ablauf einer Ungültigerklärung eines Zertifikats

Die Identifizierung und Authentifizierung bei einer Ungültigerklärung verlaufen gemäss Kapitel 3.4. Sind die Voraussetzungen für eine Ungültigerklärung eines Zertifikats erfüllt, wird das Zertifikat unverzüglich widerrufen.

Der Prozess läuft folgendermassen ab:

- Der Zertifikatsinhaber richtet den Antrag für die Ungültigerklärung an die Registrierungsstelle, die den Identifikationsprozess durchführte.
- Die Registrierungsstelle überprüft die Identität des Antragstellers und die Begründung für die Ungültigerklärung.
- Wird festgestellt, dass ein gültiger Grund für die Ungültigerklärung vorliegt, wird das Zertifikat durch Swisscom für ungültig erklärt.
- Swisscom aktualisiert die Sperrinformationen (OCSP) mit den ungültig erklärten Zertifikaten.
- Swisscom bestätigt dem Zertifikatsinhaber die Ungültigerklärung des Zertifikats.

Die Ungültigerklärung eines Zertifikats kann nicht rückgängig gemacht werden.

4.9.5 Fristen

Der Zertifikatinhaber muss unverzüglich die Registrierungsstelle benachrichtigen, die den Identifikationsprozess durchführte, und die Ungültigerklärung des eigenen Zertifikats veranlassen, wenn Gründe für eine Ungültigerklärung gemäss Kapitel 4.9.2 vorliegen.

4.9.6 CRL

Die CRL für die Root CAs werden bei Bedarf, jedoch mindestens einmal im Jahr aktualisiert (Frequenz). Nach einer Veränderung wird eine CRL innerhalb von spätestens 12 Stunden veröffentlicht (Latenz).

Die URL, unter der die zugehörige Sperrliste bzw. OCSP veröffentlicht wird, ist im Zertifikat aufgeführt.

Die Statusinformationen sind mindestens 11 Jahre über die Laufzeit des Zertifikates hinaus im Verzeichnisdienst verfügbar.

4.9.7 Suspendierung

Swisscom nimmt keine Suspendierung (zeitliche Aussetzung) von Zertifikaten vor.

4.10 Dienst zur Statusabfrage von Zertifikaten

Swisscom stellt eine CRL für die Root CAs und einen OCSP-Dienst für die Issuing CAs und die TSS CA zur Verfügung, womit der Status, (insbesondere die Gültigkeit) aller ausgestellten Zertifikate überprüft werden kann. Details zur Verfügbarkeit sind dem Kapitel 2.1 zu entnehmen. Details zu den bereitgestellten Diensten sind im [Addendum] beschrieben.

Die Daten in OCSP werden jeweils sofort nach einer Änderung aktualisiert.

4.11 Beendigung des Vertragsverhältnisses durch den Zertifikatinhaber

Die Dauer des Vertragsverhältnisses und die Beendigungsmöglichkeiten durch den Zertifikatsinhaber ergeben sich aus den jeweils anwendbaren Vertragsbestimmungen (wie zum Beispiel aus den Nutzungsbestimmungen der jeweiligen Zertifikatsklasse).

4.12 Schlüsselhinterlegung und -wiederherstellung

Swisscom bietet keine Schlüsselhinterlegung und –Wiederherstellung (Key-Escrow and Recovery) für die Zertifikatsinhaber an.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen

Einzelne Richtlinien, wie zum Beispiel das Rollenkonzept oder die Zutritts-Policy, liegen in eigenständigen Dokumenten vor, die nicht veröffentlicht werden, jedoch bei Swisscom zur Einsicht angefordert werden können.

5.1 Infrastrukturelle Sicherheitsmassnahmen

5.1.1 Lage und Konstruktion

Die PKI-Systeme der Swisscom befinden sich in Trust Centern. Die wichtigen Komponenten sind redundant ausgelegt und befinden sich in zwei getrennten Rechenzentren von Swisscom in der Schweiz.

Die Trust Center bieten hinsichtlich der infrastrukturellen Sicherheitsmassnahmen einen ausreichenden Schutz und entsprechen den gesetzlichen Vorschriften.

5.1.2 Zutrittskontrolle

Die Trust Center sind durch geeignete technische und infrastrukturelle Massnahmen gesichert, so dass nur berechtigte Mitarbeiter Zutritt haben, die eine Rolle innerhalb der Betriebsorganisation wahrnehmen und autorisiert wurden. Der Zutritt zum Trust Center ist durch eine Zutrittsanlage geschützt.

5.1.3 Stromversorgung und Klimatisierung

Die Rechenzentren der Swisscom verfügen über eine unterbruchsfreie Stromversorgung (no-break). Bei Stromausfällen wird Strom von einem Notstromaggregat produziert.

In den Trust Centern sorgen redundant ausgelegte Klimaanlagen für eine geeignete Raumtemperatur und Luftfeuchtigkeit.

5.1.4 Abwehr von Wasserschäden

Die Serverräume für die technische Infrastruktur verfügen über einen angemessenen Schutz vor Wasserschäden.

5.1.5 Feuer

Es bestehen Brandschutzvorschriften. Insbesondere verfügen die Trust Center über Brandmeldeanlagen und Handfeuerlöscher in ausreichender Anzahl.

5.1.6 Datenträger

Datenträger werden in verschlossenen Räumen oder Schränken aufbewahrt. Sofern Datenträger mit sensiblen Daten sich nicht in einem Rechenzentrum der Swisscom befinden, werden sie in einem Tresor aufbewahrt.

5.1.7 Abfallentsorgung

Sämtliche Daten auf elektronischen Datenträgern oder Papier werden fachgerecht vernichtet und anschliessend entsorgt.

5.1.8 Externes Backup

Die Backups der Systeme werden in zwei verschiedenen Swisscom Rechenzentren in der Schweiz aufbewahrt.

5.2 Organisatorische Sicherheitsmassnahmen

5.2.1 Vertrauenswürdige Rollen

Vertrauenswürdige Rollen müssen von Personen übernommen werden, die ihrer Rolle entsprechend geschult wurden. Solche Personen können Swisscom Mitarbeiter oder Vertragspartner sein. Sie haben Zugriff auf die Systeme der Swisscom PKI und führen Identitätsüberprüfungen oder kryptographische Operationen aus, die wesentliche Auswirkungen haben können auf:

- Die Validierung von Informationen in Zertifikatsanträgen
- Die Annahme, Ablehnung oder sonstige Verarbeitung von Zertifikatsanträgen
- Sperranträge oder Enrollment Informationen
- Die Ausgabe oder den Widerruf von Zertifikaten
- die Handhabung der Informationen oder Anfragen der Zertifikats-Besteller.

Vertrauenswürdige Personen umfassen, sind aber nicht beschränkt auf:

- Administratoren von kryptographischen Systemen
- System-Administratoren
- Engineers
- Information Security Officer
- zuständige Führungskräfte

Die Aufgaben und Pflichten von Personen in vertrauenswürdigen Rollen werden so verteilt, dass eine Person nicht allein handeln und so die Sicherheitsmassnahmen umgehen und die Vertrauenswürdigkeit der PKI oder TSA-Operationen untergraben kann.

5.2.2 Anzahl erforderlicher Mitarbeiter pro Aufgabe

Kryptografische Devices wie HSM und CA-Server sind besonderen Authentisierungsverfahren unterworfen. Für alle Zugriffe auf diese Systeme wird das „4-Augen-Prinzip" durch technische oder organisatorische Massnahmen (z.B. Verwendung von verschiedenen PED-keys) erzwungen.

5.2.3 Identifizierung und Authentisierung der Rollen

Die Identifizierung und Authentisierung der Rollen ist im [Rollenkonzept] der Swisscom PKI beschrieben. Der technische Zugang zu den einzelnen IT-Systemen wird durch starke Authentisierung oder Benutzerkennung und Passwort realisiert.

5.2.4 Trennung von Aufgaben

Das [Rollenkonzept] sieht eine Trennung der Aufgaben vor, um die Ansammlung von unverträglichen Rollen auf einer Person zu unterbinden und somit Interessenskonflikte zu verhindern, das "4-Augen-Prinzip" durchzusetzen und schadendes Verhalten vorzubeugen.

5.3 Personelle Sicherheitsmassnahmen

5.3.1 Anforderungen an die Mitarbeiter

Die Mitarbeiter von Swisscom, welche für den Betrieb der Plattform oder die Überwachung zuständig sind, erfüllen die gesetzlichen Anforderungen, insbesondere hinsichtlich Fachwissen, Zuverlässigkeit, Erfahrung und Qualifikationen.

Neben einer allgemeinen Ausbildung auf dem Gebiet Informationstechnik verfügen die Mitarbeiter in ihrer Rolle über angemessene Fachkenntnisse in den Bereichen:

- EDV allgemein,
- Sicherheitstechnologie, Kryptographie, elektronische Signatur und PKI,
- technische Normen, insbesondere Evaluierungsnormen,
- Hard- und Software,
- Vorschriften für die Sicherheit und den Schutz personenbezogener Daten,
- Anwendung von Verwaltungs- und Managementverfahren.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Von Mitarbeitern mit Zugriff auf die Swisscom CA liegt vor:

- Strafregisterauszug
- Betreibungsregisterauszug.

5.3.3 Anforderungen an die Schulung

In der Betriebsorganisation der Swisscom PKI werden ausschliesslich qualifizierte Mitarbeiter eingesetzt.

Ein Mitarbeiter erhält erst nach Nachweis der notwendigen Fachkunde eine Berechtigung, eine spezifische Rolle auszuführen.

Schulungen werden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und Sicherheitstechnik durchgeführt. Zusätzlich werden alle Mitarbeiter von Swisscom regelmäßig (mindestens alle 12 Monate) zu neuen Bedrohungen und aktuellen Sicherheitspraktiken geschult.

5.3.4 Sanktionen für unautorisierte Handlungen

Unautorisierte Handlungen, die die Sicherheit der IT-Systeme der Swisscom PKI gefährden oder gegen Datenschutzbestimmungen verstossen, werden disziplinarisch geahndet.

5.3.5 Dokumente für die Mitarbeiter

Den Mitarbeitern der Swisscom PKI stehen Schulungsunterlagen, Betriebsdokumente und Verfahrensanweisungen im Intranet Swisscom zur Verfügung.

5.4 Sicherheitsüberwachung

5.4.1 Überwachte Ereignisse

Folgende Ereignisse werden protokolliert:

- Serverrelevante Ereignisse wie Zugriffsversuche, System Startup und Shutdown, Systemabstürze, Hardware Fehler sowie Änderungen an der Software und der Konfiguration
- Alle Tätigkeiten auf den CAs, wie die Signierung und Revokation von Zertifikaten, CRL-Generierung, etc.
- In- und Ausserbetriebnahme von kryptografischen Komponenten
- Änderungen der CP/CPS
- Zutritte zu den Serverräumen, technische Alarme und Einbruchmeldungen

Jedes protokollierte Ereignis wird mit einem Zeitstempel versehen und die durchführende Person bzw. der durchführende Prozess wird angegeben.

5.4.2 Schutz der Protokolldaten

Die Protokolldaten werden auf einen zentralen Log-Server übertragen und dort gegen Zugriff, Löschung und Manipulation geschützt.

5.5 Archivierung

5.5.1 Archivierte Daten

Archiviert werden alle Daten, die für den Zertifizierungsprozess relevant sind:

- Zertifikatanträge inkl. Identitäts- und Vertretungsnachweisen
- Zustimmung zu den Nutzungsbestimmungen
- Anträge auf Ungültigerklärung
- sämtliche Ereignisse, die den Lebenszyklus der von Swisscom verwalteten bzw. ausgestellten privaten kryptografischen Schlüssel betreffen

Des Weiteren werden u.a. folgende Daten archiviert:

- Verträge
- Tätigkeitsjournal der Swisscom PKI

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Die Aufbewahrungsdauer für archivierte Daten ist in Kapitel 3.2 beschrieben.

5.5.3 Schutz der Archive

Es wird durch geeignete Massnahmen sichergestellt, dass die Daten weder unbefugt gelesen oder kopiert sowie weder verändert noch gelöscht werden können.

Der ISO kann den Abruf und die Prüfung der archivierten Daten autorisieren.

5.6 Schlüsselwechsel

Bei dem Schlüsselwechsel einer CA wird ein neues Zertifikat erstellt und gemäss Kapitel 2.2 publiziert. Sollte der Schlüsselwechsel eine Root-CA betreffen, wird zusätzlich ein neues Zertifikat mit dem alten privaten kryptografischen Schlüssel signiert und publiziert.

Falls ein privater kryptografischer Schlüssel einer CA kompromittiert wurde, gelten die Regelungen in Kapitel 5.7.3.

5.7 Kompromittierung und Wiederherstellung

5.7.1 Prozeduren bei Sicherheitsvorfällen und Kompromittierung

Die Prozeduren zur Behandlung von Sicherheitsvorfällen und bei der Kompromittierung von privaten kryptografischen Schlüsseln einer CA sind dokumentiert. Diese Prozeduren sind den beteiligten Rollen bekannt und werden bei Bedarf entsprechend ausgeführt.

5.7.2 Wiederherstellung von IT-Systemen

Swisscom wendet umfassende und wirksame Prozeduren zum Erkennen und Behandeln von Incidents und Schwachstellen an.

5.7.3 Kompromittierung von privaten kryptografischen Schlüsseln einer CA

Wurde der private kryptografische Schlüssel einer CA kompromittiert oder besteht ein begründeter Verdacht auf eine Kompromittierung, so werden folgende Massnahmen ergriffen:

- Widerruf des betroffenen CA-Zertifikats sowie aller noch gültiger Zertifikate, die von dieser CA ausgestellt wurden
- Information betroffener Zertifikatsinhaber

Anschliessend an eine Untersuchung der Vorkommnisse werden, unter Berücksichtigung der Gründe für die Kompromittierung, neue CA-Schlüssel generiert und neue CA-Zertifikate ausgestellt.

5.7.4 Betrieb nach einer Katastrophe

Eine Wiederaufnahme des Zertifizierungsbetriebs nach einer Katastrophe oder nach einer Kompromittierung ist Bestandteil der Notfallplanung und kann erfolgen, sofern die Sicherheit der Zertifizierungsdienstleistung gewährleistet ist.

5.8 Einstellung des Betriebes

Bei Einstellung des Zertifizierungsbetriebes werden folgende Massnahmen ergriffen:

- Die Zertifikatsinhaber werden von der Einstellung der Tätigkeit sowie vom Widerruf, der Übernahme oder der Weiterführung verständigt;
- Archivierung der endgültigen Certificate Revocation Lists (CRL), des Transaktionsjournals sowie der Registrierungsinformationen;
- Sichere Zerstörung aller privaten kryptografischen Schlüssel der Swisscom PKI inkl. der Schlüssel-Backups.

6 Technische Sicherheitsmassnahm

6.1 Schlüsselerzeugung und Installation

6.1.1 Schlüsselerzeugung

Die Schlüsselpaare der Root-CA werden auf einem dedizierten HSM erzeugt und gespeichert. Das IT System, welches die Root-CA enthält, ist nicht an ein Netzwerk angeschlossen. Die Root-CA sowie das zugehörige HSM befinden sich im Hochsicherheitsbereich des Trust Centers. Die Prozedur zur Erzeugung von Root-CA-Schlüsseln wird von einem unabhängigen Auditor überwacht.

Die Schlüsselpaare der Issuing CAs werden in einem separaten HSM erzeugt und gespeichert.

Die HSM sind so gelagert, dass bei der Schlüsselerzeugung das 4-Augen-Prinzip durch organisatorische Massnahmen erzwungen wird. Die Erstellung von CA-Schlüsseln wird dokumentiert.

6.1.2 Übermittlung des privaten kryptografischen Schlüssels an den Zertifikatsinhaber

Die Zertifikatsübermittlung bei Schlüsselgenerierung durch die Swisscom ist in Kapitel 4.3 beschrieben.

6.1.3 Auslieferung des öffentlichen kryptografischen CA-Schlüssels

Alle Teilnehmer der Swisscom PKI können die öffentlichen kryptografischen Schlüssel (public key) der Swisscom Root-CA und der untergeordneten CAs über den Verzeichnisdienst (siehe Kapitel 2.1) abrufen.

6.1.4 Algorithmen und Schlüssellängen

Die eingesetzten kryptografischen Algorithmen und deren Schlüssellängen orientieren sich an den Veröffentlichungen der ETSI und sind mindestens:

- RSA 4096 SHA-256 für Root-Keys
- RSA 2048 SHA-256 für die CAs der nachfolgenden Stufe (Level 1) und die TSA
- Für End-Entity-Zertifikate und Time-stamping
    - RSA 2048 SHA-256
    - ECC 256 NIST-P256r1

6.1.5 Parameter der öffentlichen kryptografischen Schlüssel und Qualitätssicherung

Die CA-Zertifikate und die Zertifikate der Klasse "Rubin" werden auf Grundlage von Schlüsseln ausgestellt, die [ETSI TS 119 312] in der aktuell gültigen Fassung entsprechen.

6.1.6 Verwendungszweck der Schlüssel und Beschränkungen

Der Verwendungszweck der Schlüssel und allfällige Beschränkungen werden im entsprechenden X.509 v3 Feld (keyUsage) festgelegt (siehe [Addendum] zum CP/CPS, Kapitel 2).

6.2 Schutz des privaten kryptografischen Schlüssels

Während des gesamten Lebenszyklus (einschließlich Lieferung und Lagerung) werden die HSM-Module durch technische und organisatorische Maßnahmen vor unautorisiertem Zugriff geschützt.

6.2.1 Standard der kryptografischen Module

Die eingesetzten HSM-Module sind mindestens FIPS 140-2 Level 3 konform.

Der Zertifizierungsstatus der eingesetzten HSM-Module wird während ihres gesamten Lebenszyklus überwacht. Im Falle der Änderung des Zertifizierungsstatus wird Swisscom eine Impact Analyse durchführen und anschliessend die erforderlichen Massnahmen festlegen.

6.2.2 Teilung des privaten kryptografischen Schlüssels

Eine Teilung der privaten kryptografischen Schlüssel der Swisscom Root-CA und der Issuing CAs ist nicht vorgesehen.

6.2.3 Hinterlegung privater kryptografischer Schlüssel

Private kryptografische Schlüssel von Zertifikatsinhabern werden nicht hinterlegt.

6.2.4 Backup der privaten kryptografischen Schlüssel

Von den Schüsselpaaren der Root-CA und der Issuing CAs werden Kopien angefertigt und auf einem HSM in einem Safe aufbewahrt. Für das Backupsystem gelten die gleichen Voraussetzungen und Sicherheitsmassnahmen wie für das Produktivsystem.

6.2.5 Archivierung der privaten kryptografischen Schlüssel

Private kryptografische Schlüssel von Root CA, Issuing CAs oder Zertifikatsinhabern werden von Swisscom nicht archiviert.

6.2.6 Erstellung und Speicherung privater Schlüssel

Die privaten Schlüssel von Root CA und Issuing CAs werden ausschliesslich in HSMs erstellt und gespeichert.

6.2.7 Aktivierung der privaten kryptografischen Schlüssel

Die privaten kryptografischen Schlüssel der CAs können nur im 4-Augen-Prinzip von Personen in den entsprechenden vertrauenswürdigen Rollen aktiviert werden.

Zertifikatsinhaber generieren und verwalten ihre privaten kryptografischen Schlüssel in der Regel selbst. Bei Schlüsselaufbewahrung durch Swisscom erhält der Zertifikatsinhaber nach erfolgreicher Registrierung persönliche Aktivierungsdaten, die zur Freigabe des privaten kryptografischen Schlüssels eingesetzt werden müssen.

6.2.8 Deaktivierung der privaten kryptografischen Schlüssel

Die privaten kryptografischen Schlüssel der CAs werden durch Beendigung der Verbindung zwischen HSM und der Management Software deaktiviert.

Zertifikatsinhaber löschen ihre privaten kryptografischen Schlüssel oder die persönlichen Aktivierungsdaten zur Freigabe des privaten kryptografischen Schlüssels nach Bedarf selbst.

6.2.9 Vernichtung der privaten kryptografischen Schlüssel

Bei der Vernichtung der privaten Schlüssel der Root-CA und der ihr nachgelagerten Issuing CAs wird nach dem vier-Augen-Prinzip verfahren. Das Verfahren wird protokolliert.

Zertifikatsinhaber vernichten ihre privaten kryptografischen Schlüssel oder die persönlichen Aktivierungsdaten zur Freigabe des privaten kryptografischen Schlüssels nach Bedarf selbst.

6.2.10 Güte des kryptografischen Moduls

Swisscom betreibt geeignete hard- und softwarebasierte Schlüsselgeneratoren, um die Qualität des Schlüssel-Materials sicherzustellen.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher kryptografischer Schlüssel

Öffentliche kryptografische Schlüssel werden sowohl im Verzeichnisdienst als auch auf Medien für die Datensicherung archiviert.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Die von der Root-CA und den Issuing CAs ausgestellten Zertifikate haben folgende Gültigkeitszeiträume:

- Zertifikat der Root-CA maximal 20 Jahre
- Zertifikate der Issuing CAs maximal 10 Jahre
- Zertifikate der Klasse „Rubin“ maximal 3 Jahre

Die effektive Gültigkeitsdauer der Schlüssel und Zertifikate sind dem Zertifikat zu entnehmen.

6.4 Aktivierungsdaten

6.4.1 Aktivierungsdaten für Schlüssel von natürlichen Personen

Zertifikatsinhaber verwalten die Aktivierungsdaten für den Zugriff auf ihre privaten kryptografischen Schlüssel selbst. Es werden keine Richtlinien erzwungen.

6.4.2 Aktivierungsdaten für Schlüssel von Organisationen

Zertifikatsinhaber verwalten die Aktivierungsdaten für den Zugriff auf ihre privaten kryptografischen Schlüssel selbst. Es werden keine Richtlinien erzwungen.

6.4.3 Aktivierungsdaten für CA Schlüssel

Die Aktivierung der Schlüssel der Root CA und der Issuing CAs im HSM erfordert die Beteiligung von zwei Personen in vertrauenswürdigen Rollen (siehe Kapitel 5.2.1).

6.5 Sicherheitsmassnahmen für Devices

6.5.1 Spezifische Anforderungen an technische Sicherheitsmassnahmen

Bei der Swisscom PKI eingesetzte Computer, Proxies und andere Komponenten werden einer Risikoanalyse unterzogen und ihrem Gefährdungspotential entsprechend abgesichert.

Darüber hinaus werden folgende Sicherheitsmassnahmen umgesetzt:

- Restriktive Zugriffskontrolle
- Benutzerauthentisierung und -autorisierung erfolgt nach den „need-to-know“ und „need-to-do“ Prinzipien
- Perimeterschutz: Virenschutz, Einsatz von Firewall Kaskaden und Web Application Firewall (WAF).
- Einsatz von aktuellen Software-Releases und zeitnahe Installation von sicherheitsrelevanten Software-Updates

6.5.2 Güte /Qualität der Sicherheitsmassnahmen

Die Sicherheitsmassnahmen werden periodisch überprüft.

6.6 Lebenszyklus der Sicherheitsmassnahmen

6.6.1 Softwareentwicklung

Der Einsatz von Software (Eigen- oder Fremdentwicklung) erfolgt erst nach Abnahme und Freigabe.

6.6.2 Sicherheitsmanagement

Das Sicherheitsmanagement umfasst folgende Aspekte:

- Audits nach ETSI EN 319 401 und ETSI EN 319 411-1
- Regelmässige Evaluierung und Weiterentwicklung des Sicherheitskonzepts
- Überprüfung der Sicherheit im laufenden Betrieb (siehe auch Kapitel 5.4)
- Logging aller sicherheitsrelevanten Vorgänge
- Zusammenarbeit mit dem Swisscom-Computer Security Incident Response Team (CSIRT)
- Einspielung von Upgrades und Patches
- Einsatz von Upgrades oder Patches auf einem Produktivsystem erst nach Freigabe auf einem Testsystem.

6.7 Sicherheitsmassnahmen für das Netzwerk

Das Netzwerk der CA ist in verschiedene Sicherheitszonen unterteilt, die jeweils durch eine Firewall voneinander abgeschottet sind. Sämtliche Assets (Devices, Schlüsselmaterial und Informationen) werden klassifiziert und in der Sicherheitszone platziert, die ihrer Klassifizierung entspricht.

Das Management-Netzwerk ist vom Daten-Netzwerk abgetrennt.

Kritische Sicherheitsvorfälle werden unverzüglich in Zusammenarbeit mit dem Swisscom-CSIRT verfolgt und bearbeitet.

6.8 Zeitstempel

Swisscom betreibt einen internen Zeitservice. Für die Zeitbasis werden zwei verschiedene externe Zeitsignale korreliert, um sicherzustellen, dass die interne Zeit mit der koordinierten Weltzeit (UTC) synchron ist. Die Zeitbasis wird über das Network Time Protocol (NTP) auch an alle Server der Swisscom PKI verteilt.

Basierend auf diesem internen Zeitservice stellt Swisscom einen qualifizierten Zeitstempeldienst gemäss Art. 2 Bst. j [ZertES] zur Verfügung.

7 Profile für Zertifikate, Sperrlisten (CRL) und Online-Statusabfragen

Die Zertifikatsprofile, Widerrufslisten (CRL) und Online-Statusabfragen (OCSP) entsprechen dem Standard X.509 v3, den Vorgaben von [RFC 5280] sowie [RFC 6960]. Sie sind im [Addendum] zu dieser CP/CPS detailliert beschrieben.

8 Konformitätsprüfung (Compliance Audit) und andere Assessments

8.1 Konformität

Die Services, Prozesse und Sicherheitsmassnahmen basieren auf den folgenden Gesetzen und Regularien:

- diese CP/CPS sowie zugehörige Dokumente wie Sicherheitskonzept, Rollenkonzept etc.
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI);
  General Policy Requirements for Trust Service Providers [ETSI EN 319 401] (2018-04)
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI);
  Policy and security requirements for Trust Service Providers issuing certificates;
  Part 1: General requirements [ETSI EN 319 411-1] (2018-04)

8.2 Zertifizierung

Die Einhaltung der in Kap. 8.1 aufgeführten Standards wird regelmässig überprüft und zertifiziert.

Zertifizierungsdienste auf der Basis von fortgeschrittenen Zertifikaten (Zertifikatsklasse Rubin) sind in der Schweiz gesetzlich nicht geregelt.

8.3 Intervall und Umstände der Überprüfung

Ein externer Auditor überprüft Swisscom sowie Registrierungsstellen in regelmässigen Abständen sowie nach sicherheitsrelevanten Veränderungen der CP/CPS.

8.4 Überprüfte Bereiche

Die von einer Überprüfung betroffenen Bereiche entsprechen den Anforderungen der unter 8.1 aufgeführten Standards. Für Risiken, die zwingend eine Überprüfung notwendig machen, können bestimmte Bereiche im Voraus festgelegt werden.

8.5 Mängelbeseitigung

Aufgedeckte Mängel werden in Abstimmung mit den Registrierungsstellen kategorisiert und gegebenenfalls behoben.

9 Rahmenbestimmungen

9.1 Vergütung

Die Vergütung wird in den jeweiligen Verträgen mit Swisscom vereinbart (z.B. im Vertrag zwischen Swisscom und RA-Partner).

9.2 Haftpflichtversicherung von Swisscom

Swisscom verfügt über eine Haftpflichtversicherung im Sinne des [VZertES].

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertraulich zu behandelnde Daten

Informationen über Beteiligte gemäss Kapitel 1.3, die nicht unter Kapitel 9.3.2 fallen, gelten als vertrauliche Informationen. Zu diesen Informationen zählen u.a. Geschäftspläne, Informationen über Geschäftspartner und ebenso alle Informationen, die im Registrierungsprozess erfasst werden.

9.3.2 Nicht vertraulich zu behandelnde Daten

Als nicht vertraulich gelten Informationen, die in den Zertifikaten und der Liste der für ungültig erklärten Zertifikate enthalten sind (z.B. Elemente des DN).

9.3.3 Verantwortung für den Schutz vertraulicher Informationen

Swisscom trägt die Verantwortung für Massnahmen zum Schutz vertraulicher Informationen. Daten dürfen nur im Rahmen der Diensterbringung bearbeitet und an Dritte nur weitergegeben werden, wenn zuvor die Vertraulichkeit vertraglich sichergestellt worden ist. Nicht als Dritte gelten die RA-Partner, die im Rahmen der Bearbeitung des Zertifikatantrages Daten an Swisscom weitergeben können und an die Swisscom wiederum die bearbeiteten Daten weitergeben kann. Zu Audit- oder Revisionszwecken können Dokumente im Beisein des Information Security Officers von Swisscom eingesehen werden.

9.4 Schutz von Personendaten (Datenschutz)

9.4.1 Allgemein

Swisscom erhebt, speichert und bearbeitet nur Daten, die für die Erbringung der Leistungen, für die Abwicklung und Pflege der Kundenbeziehung, namentlich die Gewährleistung einer hohen Leistungsqualität, für die Sicherheit von Betrieb und Infrastruktur sowie für die Rechnungsstellung benötigt werden.

Swisscom (Schweiz) AG betreibt die IT-Systeme zur Erbringung der Zertifizierungsdienste und diese Systeme stehen in der Schweiz. Die digitalen Zertifikate werden somit in der Schweiz ausgestellt.

9.4.2 Verantwortlicher Umgang mit Personendaten

Swisscom und ihre RA-Partner halten sich an das Datenschutzgesetz und insbesondere an folgende Grundsätze:

- Personendaten dürfen nur rechtmässig beschafft werden.
- Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.

- Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

9.4.3 Offenlegung gegenüber Gerichten und anderen Behörden

Swisscom Auskunfts- und Mitwirkungspflichten gegenüber Gerichten und anderen Behörden bleiben von den Regelungen dieser CP/CPS und von konkreten vertraglichen Regelungen unberührt. Swisscom hat insbesondere Daten der Zertifikatsinhaber an Gerichte und andere Behörden in Übereinstimmung mit den geltenden Gesetzen zu übergeben.

9.4.4 Andere Umstände einer Weitergabe von Daten an Dritte

Verwendet der Zertifikatsinhaber im Zertifikat ein Pseudonym, hat Swisscom die Daten über die Identität des Zertifikatsinhabers zu übermitteln, sofern an der Feststellung der Identität ein überwiegendes berechtigtes Interesse glaubhaft gemacht wird.

9.5 Urheberrechte

Swisscom ist Urheberin der folgenden Dokumente:

- vorliegende CP/CPS;
- dazugehörige Nutzungsbestimmungen.

Swisscom räumt den RA-Partnern und den Zertifikatsinhabern das Recht ein, die genannten Dokumente unverändert an Dritte weiter zu geben. Weitergehende Rechte werden nicht eingeräumt. Insbesondere sind die Weitergabe veränderter Fassungen und die Überführung in andere Dokumente oder Publikationen ohne vorgängige schriftliche Zustimmung von Swisscom nicht zulässig.

Swisscom räumt der Mozilla Foundation ein Nutzungsrecht an dieser CP/CPS gemäss der Creative Commons Lizenz "CC BY-ND 4.0" (Attribution-NoDerivatives 4.0 International) ein, soweit dies in Anwendung der "Mozilla Root Store Policy" der Mozilla Foundation notwendig ist.

9.6 Gewährleistung

9.6.1 Gewährleistung von Swisscom

Swisscom gewährleistet, dass die Angaben im Zertifikat den im Authentifikationsprozess gemäss diesem Dokument gewonnen Informationen entsprechen.

9.6.2 Gewährleistungen anderer Beteiligter

Weitere Gewährleistungen werden in den jeweiligen Verträgen mit Swisscom geregelt.

RA-Partner haben insbesondere zu gewährleisten, dass sie die an sie gestellten Anforderungen gemäss diesem Dokument und gemäss anwendbarer Signaturgesetzgebung erfüllen.

9.7 Haftung

9.7.1 Haftung von Swisscom

Die Haftung von Swisscom nach den vertraglichen Vereinbarungen. Sofern die vertraglichen Vereinbarungen keine andere Haftungsregelung enthalten, haftet Swisscom wie folgt: Bei Vertragsverletzungen haftet Swisscom für den nachgewiesenen Schaden, sofern sie nicht beweist, dass sie kein Verschulden trifft. Für absichtlich und grobfahrlässig verursachte Schäden sowie für Personenschaden haftet Swisscom unbegrenzt. Swisscoms Haftung für Schäden infolge leichter Fahrlässigkeit ist – soweit gesetzlich zulässig – ausgeschlossen.

9.7.2 Haftung anderer Beteiligter

Die Haftung des Zertifikatsinhabers wird in den Nutzungsbestimmungen geregelt und richtet sich nach dem jeweils anwendbaren Recht.

Die Haftung der RA-Partner ist Gegenstands des Vertrags zwischen Swisscom und dem RA-Partner.

9.8 Inkrafttreten und Aufhebung

9.8.1 Inkrafttreten

Diese CP/CPS treten an dem Tag in Kraft, an dem sie über den Informationsdienst (siehe Kapitel 2.2) von Swisscom veröffentlicht werden.

9.8.2 Aufhebung

Dieses Dokument ist gültig, bis:

- es durch eine neue Version ersetzt wird oder
- der Betrieb des Zertifizierungsdienstes von Swisscom eingestellt wird.

9.8.3 Konsequenzen der Aufhebung

Ist die Gültigkeitsdauer eines Zertifikats im Zeitpunkt der Aufhebung der vorliegenden CP/CPS bzw. im Zeitpunkt des Inkrafttretens der neuen CP/CPS noch nicht abgelaufen, gelten ab Benachrichtigung (vgl. hierzu Kapitel 9.8.4) für die verbleibende Gültigkeitsdauer die Bestimmungen der neuen CP/CPS.

Will der Zertifikatsinhaber die neue CP/CPS nicht akzeptieren, hat er auf die weitere Verwendung des Zertifikats zu verzichten. Mit der weiteren Verwendung des Zertifikats akzeptiert der Zertifikatsinhaber die neue CP/CPS.

9.8.4 Individuelle Benachrichtigungen und Kommunikation mit Zertifikatsinhabern

Die Benachrichtigung der Zertifikatsinhaber wird durch die zuständige Registrierungsstelle sichergestellt. Über die bei der Registrierung angegebene Mobiltelefonnummer bzw. E-Mail-Adresse oder alternative der Registrierungsstelle zur Verfügung stehende Kommunikationskanäle informieren diese nach eigenem Gutdünken die Zertifikatinhaber über das Inkrafttreten einer neuen Version der CP/CPS.

9.8.5 Änderungen dieses Dokuments

Änderungen an dieser CP/CPS werden in Absprache mit den Registrierungsstellen kommuniziert.

9.9 Konfliktbeilegung

Im Konfliktfall bemühen sich die Beteiligten um eine einvernehmliche Streitbeilegung.

9.10 Anwendbares Recht und Gerichtsstand

Alle Rechtsbeziehungen im Zusammenhang mit den Services von Swisscom gemäss diesem Dokument unterliegen der jeweiligen Regelung in den Verträgen (insbesondere Vertrag zischen Swisscom und RA-Partner, Vertrag zwischen Swisscom und Zertifikatsinhaber).

Falls diese Verträge keine diesbezügliche Regelung enthalten, gilt:

- Unter Vorbehalt von anderslautendem zwingendem Recht (z.B. Konsumentenschutz-bestimmungen), unterliegen alle Rechtsbeziehungen im Zusammenhang mit den Services von Swisscom gemäss diesem Dokument Schweizerischem Recht, unter Ausschluss der Kollisionsnormen des internationalen Privatrechts und das Übereinkommen der Vereinten Nationen über den internationalen Warenkauf vom 11. April 1980.

- Unter Vorbehalt von anderslautendem zwingendem Recht (z.B. Konsumentenschutzbestimmungen), ist der ausschliessliche Gerichtsstand in Bern.

9.11 Einhaltung des anwendbaren Rechts

Alle Beteiligten halten die auf sie anwendbaren Gesetze und Regularien ein.

9.12 Sprache

Die deutsche Originalversion dieses Dokuments ist rechtlich verbindlich. Daneben kann es auch Übersetzungen geben.