Zertifikatsrichtlinien (CP/CPS)
zur Ausstellung von Zertifikaten der Klassen „Diamant“ (geregelt/qualifiziert) und „Saphir“ (fortgeschritten)

Version: 3.9

Datum: 10. Oktober 2023

Swisscom (Schweiz) AG
Alte Tiefenaustrasse 6
3050 Bern

Änderungskontrolle

Version	Datum	Ausführende Stelle	Bemerkungen/Art der Änderung
3.0	30.06.2017	Kerstin Wagner, H-P Waldegger; Stéphane Vaucher	Erstellung der CP/CPS nach ZertES und den neuen ETSI-Standards.
3.0	15.08.2017	Governance Board	Freigabe
3.1	30.01.2018	Kerstin Wagner, H-P Waldegger; Stéphane Vaucher	Diverse Präzisierungen und Korrekturen;
3.1	29.01.2018	Governance Board	Freigabe
3.2	08.03.2018	H-P Waldegger	Feedback Konformitätsprüfung und Ergänzung Siegelprozesse bei Nutzung eigener HSM durch Kunden
3.2	18.04.2018	Governance Board	Freigabe
3.3	13.06.2018	Kerstin Wagner H-P Waldegger	Diverse Präzisierungen Definition der Aufbewahrungsdauer für "Saphir" in Kap. 5.5.2, CA 4 ergänzt
3.3	19.11.2018	Governance Board	Freigabe
3.4	15.03.2019	Kerstin Wagner H-P Waldegger	Ergänzung "geregelte Zertifikate", Ergänzungen zur Root CA 4 Hierarchie, entfernen der Referenzen auf die Zertifikatsklasse Smaragd; neue Time-stamping Infrastruktur
3.4	22.01.2020	QTSP Board	Freigabe
3.5	15.06.2020	H-P Waldegger Kerstin Wagner	Haftungsbeschränkungen Kap. 9.7.1 eingefügt; neue CA Hierarchien (Kap. 1.3.1)
3.5	01.07.2020	QTSP Board	Freigabe
3.6	18.01.2021	H-P Waldegger Kerstin Wagner	Zertifikatsnutzung und -publikation ergänzt.
3.6	18.01.2021	QTSP Board	Freigabe
3.7	03.06.2021	Kerstin Wagner	Korrektur der OID der Root CA2, Standorte für Backup angepasst, neue CA Hierarchie, Aktualisierung CRL und OCSP-Service, Aktualisierung und Ergänzung der Regularien
3.7	27.01.2022	QTSP Board	Freigabe
3.8	13.06.2022	Urs Würgler Kerstin Wagner	Berücksichtigung der neuen TAV-Anforderungen; Ausserbetriebnahme der Diamant CA 2 und Saphir CA 2
3.8	08.02.2023	QTSP Board	Freigabe
3.9	05.09.2023	Kerstin Wagner	Aktualisierung bez. der relevanten Standards und der Güte der eingesetzten HSM (Kap. 3.2.2)
3.9	10.10.2023	QTSP Board	Freigabe

Referenzierte Dokumente

[ZertES]	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES)
[VZertES]	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Verordnung über die elektronische Signatur, VZertES))
[TAV]	Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (TAV)
[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"
[DIN EN 419 241-1]	Trustworthy Systems supporting Server Signing; Part 1: General Security Requirements
[ETSI TS 119 312]	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[ETSI TS 119 431-1]	TSP service components operating a remote QCSD / SCDev
[ETSI TS 119 461]	Policy and security requirements for trust service components providing identity proofing of trust service subjects
[ETSI EN 319 401]	General Policy Requirements for Trust Service Providers
[ETSI EN 319 411-1]	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI EN 319 411-2]	Policy and security requirements for TSPs; Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETSI EN 319 421]	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[ETSI EN 319 412-1-5]	Certificate Profiles
[Addendum]	Addendum zum CP/CPS: Profile der Zertifikate, Sperrlisten (CRL) und Online Statusabfragen
[NB]	Nutzungsbestimmungen
[Rollenkonzept]	Rollenkonzept SDCS
[Sicherheitskonzept]	Sicherheitskonzept SDCS

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument (nachfolgend "CP/CPS") beschreibt die Certificate Policy (Zertifikatsrichtlinien, CP) und das Certification Practice Statement (Aussagen über die Zertifizierungspraktiken, CPS) von Swisscom (Schweiz) AG (nachfolgend "Swisscom" genannt) zur Ausgabe von Zertifikaten im Sinne des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, [ZertES]) und der zugehörigen Verordnung über die elektronische Signatur, [VZertES]).

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

Die vorliegende CP/CPS bezieht sich auf zwei verschiedene Zertifikatsklassen, "Diamant" für geregelte und qualifizierte Zertifikate sowie "Saphir" für fortgeschrittene Zertifikate und zudem auf zwei unterschiedliche CA Generationen. Die CAs der zweiten Generation unter der Root CA 2 sind am Ende ihres Lifecycles angelangt, während die CAs unter der Root CA 4 mit aktuellen Algorithmen und Schlüssellangen den Anforderungen der nächsten Jahre standhalten.

Wo nicht näher bezeichnet, beziehen sich die Angaben in diesem Dokument immer auf beide Zertifikatsklassen und auf beide CA Generationen.

1.1 Überblick

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

Diese CP/CPS entspricht den folgenden Standards des Europäischen Instituts für Telekommunikationsnormen für einen qualifizierten Zertifizierungsdiensteanbieter:

- [ETSI EN 319 411-1] (2021-05): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- [ETSI EN 319 411-2] (2021-11): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- [ETSI EN 319 421] (2016-03): Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

Um die internationale Zusammenarbeit mit anderen ZDA zu ermöglichen, wird diese CP/CPS ins Englische übersetzt; 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 Klassen „Diamant“ (qualifiziert/geregelt) und „Saphir“ (fortgeschritten)“	
Version:	3.9	
Object Identifier:	2.16.756.1.83.2.1	Root CA der Generation 2
	2.16.756.1.83.30.4.0	Root CA der Generation 4
	2.16.756.1.83.30.4.1	Diamant CA der Generation 4
	2.16.756.1.83.30.4.2	Saphir CA der Generation 4

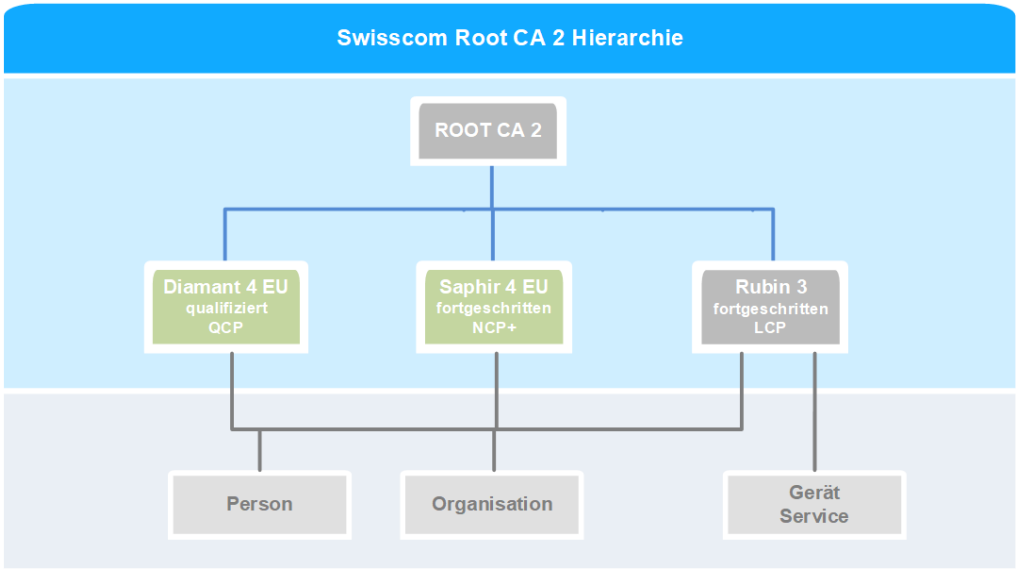
Falls Zertifikate zusätzliche Ziffern in der OID enthalten, verweisen diese auf die zum Zeitpunkt der Ausstellung gültige Versionsnummer dieses Dokuments.

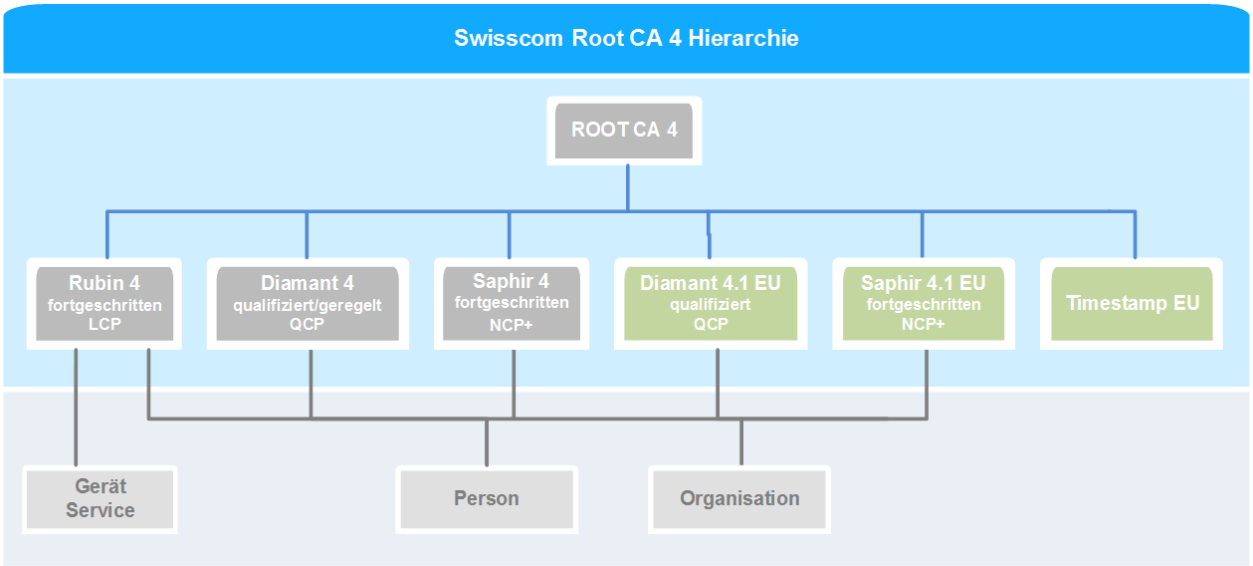
Die OID der Swisscom Digital Certificate Services basiert auf der vom schweizerischen Bundesamt für Kommunikation (BAKOM) zugeteilten RDN.

1.3 Beteiligte der PKI (nachfolgend "die Beteiligten")

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] und verwendet ein sicheres kryptografisches Gerät (HSM).

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 (HSM) 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 Service CA (qualifiziert)

Zum Erstellen und Signieren der Zertifikate der Time-Stamping Units (TSU). Entspricht der Definition für qualifizierte elektronische Zeitstempel von Art. 2 Bst. j [ZertES] sowie [ETSI EN 319 421].

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 Vertrags verpflichtet, insbesondere die in diesem Dokument definierten Prozesse für die Registrierung, Zertifikatsausgabe, Revokation und Archivierung einzuhalten.

Für jeden RA-Partner beschreibt ein Umsetzungskonzept die jeweils in ihrem Kontext eingesetzten Verfahren zur Einhaltung dieser Pflichten.

1.3.3 Zertifikatsinhaber (Subscribers)

Zertifikatsinhaber sind natürliche Personen oder UID-Einheiten, die über den im Zertifikat definierten Namen eindeutig identifiziert werden können. Der Zertifikatsinhaber ist die Person bzw. die UID-Einheit, die den privaten Schlüssel ihres Zertifikats besitzt und basierend auf diesem Zertifikat eine elektronische Signatur oder ein elektronisches Siegel erstellt.

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 (wie juristische Personen und Behörden), 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 Beteiligte

Weitere Beteiligte können natürliche Personen oder Organisationen (wie juristische Personen und Behörden) 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 stehen.[1]

Die im Rahmen dieser CP/CPS ausgestellten fortgeschrittenen Zertifikate "Saphir" können zum Erstellen von fortgeschrittenen elektronischen Signaturen durch natürliche Personen oder von fortgeschrittenen elektronischen Siegeln durch UID-Einheiten verwendet werden.

Die im Rahmen dieser CP/CPS ausgestellten Zertifikate "Diamant" können ausschliesslich wie folgt verwendet werden:

- Qualifizierte Zertifikate: zum Erstellen von qualifizierten elektronischen Signaturen durch natürliche Personen.
  Sofern die Zertifikate im Namen des Zertifikatsinhabers (siehe Kapitel 3.1)
  - die Bezeichnung "Swisscom Digital Identification and Signing" enthalten, oder
  - die Bezeichnung "Video Identifikation" enthalten, oder
  - eine Seriennummer enthalten, welche mit "DIS" oder mit "VID" startet,

  dann dürfen diese ausschliesslich im Umfeld verwendet werden, das mit der Tätigkeit des identifizierenden Finanzintermediärs eng zusammenhängt. In anderen Einsatzgebieten dürfen diese Zertifikate nicht verwendet werden.
- Geregelte Zertifikate: zum Erstellen von geregelten elektronischen Siegeln durch UID-Einheiten und Behörden.

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

Die privaten Schlüssel der Issuing CAs werden zum Signieren der zugehörigen Enduser-Zertifikate sowie TSU- 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] Die farblich hervorgehobenen Rahmen werden nachfolgend verwendet, um Regelungen einer bestimmten Zertifikatsklasse – Orange für "Diamant" und Blau für "Saphir" zuzuordnen.

Die Nutzung von Zertifikaten anderer Zertifizierungsdiensteanbieter zur Erstellung einer qualifizierten elektronischen Signatur in einem Antrag zur Ausstellung eines geregelten Zertifikats der Swisscom nach [VZertES] Art. 7 Abs. 3, ist untersagt.

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.
Benutzer/-in des Zertifikats (Relying Party)	Person oder Prozess, die oder der sich bei der Verwendung dieses Zertifikats auf die überprüften elektronischen Signaturen bzw. Siegel verlässt.
Certification 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.
Digitales Zertifikat	elektronische Bescheinigung, die einen Signaturprüfschlüssel (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 Signaturschlüssels 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.

Begriff	Erklärung
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.
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 Schlüssel. HSM werden nach Sicherheitsstandards wie z. B. FIPS 140-2 oder Common Criteria (CC) zertifiziert.
Inhaber/-in des Zertifikats (Subscriber)	Natürliche Person oder UID-Einheit, die Inhaberin des Signaturschlüssels ist, der dem im Zertifikat aufgeführten Signaturprüfschlüssel 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.
„On Demand“ Erzeugung und Nutzung von Schlüsselmaterial	„On Demand“ Erzeugung und Nutzung von Schlüsselmaterial (private und öffentliche Schlüssel sowie Zertifikate), die für die elektronische Signatur verwendet werden. Die Schlüsselpaare werden in der sicheren Umgebung des ZDA erzeugt und verwendet. Unmittelbar nach der Signaturerzeugung wird der private Schlüssel gelöscht.
QTSP (Qualified Trust Service Provider)	Geläufige englische Bezeichnung für qualifizierte Zertifizierungsdienstanbieter (ZDA).
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.

Begriff	Erklärung
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 Signaturschlüssels zugewiesen werden.
Schlüsselpaar	Signaturschlüssel und dazugehörender Signaturprüfschlüssel, 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.
Signaturprüfschlüssel (public key)	Daten wie Codes oder öffentliche kryptografische Schlüssel, die zur Überprüfung einer elektronischen Signatur oder Siegels verwendet werden.
Signaturschlüssel (private key)	Einmalige Daten wie Codes oder private kryptografische Schlüssel, die von der Inhaberin oder vom Inhaber zur Erstellung einer elektronischen Signatur oder Siegels verwendet werden.
SCD	Device für die effiziente Ausführung kryptographischer Operationen oder Applikationen. SCDs bieten einen umfangreichen Schutz privater kryptografischer Schlüssel.
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 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, Bezirken 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-

Begriff	Erklärung
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

CA	Certification Authority
CSIRT	Computer Security Incident Response Team
CN	Common Name, als Teil des DN
CP	Certificate Policy, Zertifikatsrichtlinien
CPS	Certification Practice Statement, Aussage zu den Zertifizierungspraktiken
CRL	Certificate Revocation List
DN	Distinguished Name gemäss RFC 3739
EAL	Stufe der Vertrauenswürdigkeit (Evaluation Assurance Level) nach Common Criteria
EAL4+	Anforderungen gemäss Prüfstufe EAL 4 der Norm ISO/IEC 15408-3:2008, erweitert um das Versicherungselement AVA_VAN.5 (Advanced methodical vulnerability analysis).
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
ISO	Information Security Officer, IT Sicherheitsverantwortlicher
LCP	Lightweight 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
QTSP	Qualified Trust Service Provider
RA	Registration Authority, Registrierungsstelle
Re-key	Zertifikaterneuerung mit neuen Schlüsseln
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
TLS	Transport Layer Security
TSA	Time-stamping Authority
TSP	Trust Service Provider
TSU	Time-stamping Unit
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 Root und 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 (CRL) 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 und unentgeltlich 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 oder 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 Zertifikats-inhabers ausgestellt wurde oder eine wirtschaftliche Beziehung (z.B. Bankkonto) unterhält.
Anzeige-name	commonName (CN)	Informeller Name des Zertifikatsinhabers zur allgemeinen Darstellung.	Eine Darstellung des Namens, wie es der Zertifikatsinhaber oder der ZDA zur benutzer- oder systemfreundlichen Darstellung für geeignet und verständlich hält.
Identität *entweder GN/SN*	givenName	Formale(r) Vorname(n) des Zertifikatsinhabers	Exakte Wiedergabe des Inhalts des entsprechenden Feldes aus dem vorgelegten Identitätsdokument.
	surName	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.
Eindeutigkeit	serialNumber	Abstrakte Zeichenfolge, welche die Eindeutigkeit des DN sicherstellt.	Zeichenfolge gemäss einer der folgenden Definitionen: - Von Swisscom vergebene Seriennummer - Von einer Registrierungsstelle vergebene Seriennummer mit einem spezifischen von Swisscom verwalteten Präfix - Zeichenfolge gemäss **ETSI EN 319412-2** "Natural person semantics identifier" - Vor dem 1.1.2018 verwendete Definition Bei Verwendung eines Pseudonyms oder E-Mail Adresse, welches die Eineindeutigkeit sicherstellt, kann die serialNumber weggelassen werden.

3.1.2 Für UID-Einheiten obligatorische Namensfelder

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

Der von [ETSI TS 119 461] geforderten 'attribute collection for natural person representing legal person' wird entsprochen, indem die Beantragung eines Siegels mit QES erfolgen muss.

Element	X.520 Attribut	Inhalt	Bedeutung
Land	countryName (C)	Zweistelliger ISO 3166 Ländercode	Land, in dem der Zertifikatsinhaber seinen Wohnsitz hat oder eine wirtschaftliche Beziehung (z.B. Bankkonto) unterhält oder das vorgelegte Identifikations-Dokument des Zertifikats-inhabers ausgestellt wurde.
Anzeige-name	commonName (CN)	Informeller Name des Zertifikatsinhabers zur allgemeinen Darstellung.	Eine Darstellung des Namens, wie es der Zertifikatsinhaber oder die ZDA 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 Unternehmens-Identifikationsnummer nach UIDG abgeleitete Zeichenfolge	Zeichenfolge gemäss ETSI EN 319412-3 "Legal person semantics identifier" gemäss [TAV]

3.1.3 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 sind nicht definiert. Für die Ausstellung von geregelten Zertifikaten an Behörden gelten die Format-Anforderungen der [TAV]
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.

3.1.4 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 Identifikationsmerkmal (wie Mobiltelefonnummer oder Ausweisnummer) enthalten.

3.2 Identitätsüberprüfung bei Neuantrag

Entweder der Antragsteller oder eine Person, die befugt ist, Bescheinigungen im Namen des Antragstellers anzufordern, kann ein Zertifikat anfordern. Der Antragssteller ist verantwortlich für alle Daten, die er selbst oder sein Vertreter der Swisscom zur Verfügung stellt.

3.2.1 Identifikation bei Anträgen von natürlichen Personen

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

1. Der Antragsteller muss für die Identitätsprüfung entweder einen amtlichen Lichtbildausweis oder einen anderen in seiner Zuverlässigkeit gleichwertigen, dokumentierten Nachweis erbringen. Als gleichwertig akzeptiert werden u.a.
    a. "Gelbe Identifikation" der Schweizerischen Post;
    b. POSTIDENT-Nachweis der Deutschen Post;
    c. Bestätigung der Identität eines Finanzintermediärs nach Geldwäschereigesetzes vom 10. Oktober 1997 oder eines kontoführenden Zahlungsdienstleisters, der der Payment Services Directive 2 Richtlinie (2015/2366) des Europäischen Parlaments unterstellt ist;
    d. Die Angabe eines Mobiltelefonanschlusses, der im Zusammenhang mit den Zertifizierungsdiensten eingesetzt werden soll, unter folgenden Bedingungen:
        - Der Antragsteller erbringt den Nachweis, dass er Anschlussinhaber ist bzw. sonst über den Anschluss verfügt (bei Anschlussvertrag, der auf einen anderen Namen lautet wie z. B. bei einem Geschäftstelefon);
        - Es handelt sich um einen Anschluss eines Fernmeldedienstanbieters, der dem schweizerischen Fernmelderecht untersteht;
    e. durch ein Zertifikat eines anerkannten Zertifizierungsdienstanbieters elektronisch signierte Anträge.
2. Die Registrierungsstelle überprüft die vorgelegten Dokumente und validiert ihre Übereinstimmung mit den Angaben des Gesuchs.
3. Die Registrierungsstelle führt die Identitätsprüfung anhand des vorgelegten Identitätsnachweises durch. Geprüft werden Name, Vorname und alle im Zertifikat zu vermerkenden Attribute.
4. Die Registrierungsstelle vergibt oder überprüft das Vorhandensein und die Korrektheit eines Authentisierungsmittels des Antragstellers und registriert dieses als berechtigtes Authentisierungsmittel für spätere Anpassungen der Benutzerdaten und als Methode für die Freigabe von Fernsignaturen der Swisscom.
   Das Authentisierungsmittel muss von Swisscom zugelassen sein und der in [DIN EN 419 241-1] beschriebenen Stufe 1 (Sole Control Assurance Level 1) entsprechen.

Der Antragsteller bestätigt sein Einverständnis zu dem oben beschriebenen Verfahren und die Akzeptanz der Swisscom Nutzungsbestimmungen für die entsprechende Zertifikatsklasse.

Bei Anträgen auf qualifizierte Zertifikate müssen zusätzlich folgende Vorgaben eingehalten werden:

1. Der Antragsteller muss persönlich anwesend sein oder es muss ein anderes Verfahren eingesetzt werden, das gemäss Art. 7 [VZertES] zugelassen ist oder [ETSI TS 119 461] gemäss der [TAV] erfüllt.
2. Der Antragsteller muss einen Pass oder eine für die Einreise in die Schweiz anerkannte Identitätskarte persönlich vorweisen;
3. Sofern Dokumente vorzulegen sind, müssen diese zum Zeitpunkt der ersten Identifizierung bei der Registrierung gültig sein;
4. Die Registrierung und Nutzung der Authentisierungsmittel muss mit einem Verfahren durchgeführt werden, das gemäss einer anerkannten Prüfstelle der in [DIN EN 419 241-1] beschriebenen Stufe 2 (Sole Control Assurance Level 2) entspricht. Das Verfahren darf erst nach Vorlage einer solchen Bescheinigung im Einsatz mit Fernsignaturen der Swisscom genutzt werden.

Der Zertifikatsantrag, die Identitätsnachweise und die Einwilligung zu den Nutzungsbestimmungen werden gemäss den Angaben in Kapitel 5.5.2 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 Güte für diese Person auch durch die Übersendung eines elektronisch signierten Antrags erfolgen. Voraussetzung für diese Art der Antragstellung ist, dass seit dem Erstantrag des gültigen Zertifikats nicht mehr als fünf Jahre vergangen sind und das bei der Identifizierung vorgelegte Identitätsnachweis (Pass oder Identitätskarte) gültig war.

3.2.2 Identifikation bei Anträgen von UID-Einheiten

Für die Überprüfung von Anträgen von UID-Einheiten für fortgeschrittene Zertifikate sind folgende Verfahrensschritte anwendbar:

1. Der Vertreter der Antragstellerin muss eine natürliche Person sein (auch mehrere natürliche Personen können die Vertretung gemeinsam ausüben, insbesondere bei Kollektivzeichnungsberechtigung):
    a. Bei persönlichem Erscheinen wird die Identität der Vertreter gemäss Kapitel 3.2.1 entsprechend der Anforderung der beantragten Zertifikatsklasse festgestellt.
    b. Falls der Antrag elektronisch durch die Vertreter signiert ist, wird sichergestellt, dass die verwendete Zertifikatsklasse mindestens der beantragten Zertifikatsklasse entspricht.
2. Der Vertreter der Antragstellerin hat vorzulegen:
    a. einen aktuellen Auszug aus dem Register der Registrierungsagentur, die für das betreffende Land die Organisation registriert;

b. einen von einer für die Antragstellerin zeichnungsberechtigten Person unterzeichneten Antrag.
c. Sofern die Antragstellerin nicht im Handelsregister eingetragen ist (z.B. einfache Gesellschaft, teilweise Verein), muss sie entweder den Empfang eines Briefes an der Domiziladresse nachweisen können oder die Domiziladresse durch den Besuch eines Vertreters der Swisscom bestätigen lassen.

3. Die Registrierungsstelle überprüft die vorgelegten Dokumente und validiert ihre Übereinstimmung mit den Angaben des Gesuchs (insbesondere Auszug aus dem Handelsregister).
4. Die Registrierungsstelle überprüft das Vorhandensein und die Einhaltung der technischen Mindestanforderungen des von der Antragstellerin bereitgestellten SSL/TLS-Client-Zertifikats als berechtigtes Authentisierungsmittel als Methode für die Freigabe von Fernsignaturen der Swisscom.
5. Die Antragstellerin bestätigt ihr Einverständnis zu dem oben beschriebenen Verfahren und die Akzeptanz der Swisscom Nutzungsbedingungen für die entsprechende Zertifikatsklasse.

Bei Anträgen auf geregelte Zertifikate müssen folgende zusätzliche Vorgaben eingehalten werden:

1. Der Vertreter der Antragstellerin
   - muss persönlich anwesend sein oder
   - unterzeichnet den Antrag mit einer qualifizierten elektronischen Signatur (Swisscom Diamant)

5. oder es muss ein Verfahren eingesetzt werden, dass von einer Konformitätsbewertungsstelle gemäss Art. 7 [VZertES] zugelassen ist oder [ETSI TS 119 461] gemäss der [TAV] erfüllt.

2. Der Vertreter der Antragstellerin, die eine UID-Einheit sein muss, hat vorzulegen:
   a. Falls die Antragstellerin im Handelsregister (oder ähnlichem Register) eingetragen ist: einen aktuellen und beglaubigten Auszug aus dem Handelsregister (oder gleichwertigem Register).
   b. Falls die UID-Einheit der Veröffentlichung ihrer Daten zu den Kernmerkmalen im UID-Register nicht zugestimmt hat (Art. 11 Abs. 3 UIDG): einen aktuellen und beglaubigten Auszug aus dem UID-Register.
   c. Sofern er nicht selbst im Handelsregister als allein zeichnungsberechtigt eingetragen ist: eine schriftliche Vollmacht zum Stellen eines Zertifikat-Antrags, ausgestellt vom geschäftsführenden Organ der Antragstellerin (z.B. Vorstand oder Geschäftsführung) oder von zwei im Handelsregister als zeichnungsberechtigt eingetragenen Personen. Einzelunterschrift wird nur akzeptiert, wenn Einzelzeichnungsberechtigung im Handelsregisterauszug vermerkt ist.
   d. Sofern die Antragstellerin nicht im Handelsregister eingetragen ist (z.B. einfache Gesellschaft, teilweise Verein): eine schriftliche Vollmacht zum Stellen eines Zertifikat-Antrags, ausgestellt vom obersten Organ der Antragstellerin (z.B. Vorstand oder Geschäftsführer).
   e. Die Registrierung und Nutzung der Authentisierungsmittel muss mit einem vom Antragssteller beschriebenen Verfahren durchgeführt werden, das von Swisscom zugelassen ist und der in [DIN EN 419 241-1] beschriebenen Stufe 2 (Sole Control Assurance Level 2) entspricht.

Der Zertifikatsantrag, die Vertretungsnachweise und die Einwilligung zu den Nutzungsbestimmungen werden gemäss den Angaben in Kapitel 5.5.2 aufbewahrt.

Falls die Antragstellerin selbst im Besitz des privaten Signatur-Schlüssels bleiben will, muss sie zusätzlich nachweisen, dass sowohl die Schlüsselgenerierung wie auch die Aufbewahrung und Nutzung des privaten Schlüssels ausschliesslich in einem System stattfindet, das eines der folgenden Kriterien erfüllt:

- zertifiziertes System gemäss den Anforderungen in Dokument FIPS 140-2 Stufe 3 oder höher oder gemäss den Anforderungen in Dokument FIPS 140-3 Stufe 3 oder höher;
- System, das nach der Prüfstufe EAL 4+ der Norm ISO 15408-3:2008 oder gemäss gleichwertigen anerkannten Prüfungskriterien im Sicherheitsbereich, geprüft wurde.

Dazu hat die Antragstellerin ein entsprechendes Zertifikat der eingesetzten Hardware sowie eine schriftliche Bestätigung der vorschriftsgemässen Durchführung der Schlüsselgenerierung, -aufbewahrung und -nutzung durch die Anerkennungsstelle oder eines Vertreters der Swisscom RA vorzulegen.

3.2.3 Nicht überprüfte Informationen

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

3.2.4 Verfahren zur Überprüfung des Besitzes des privaten Schlüssels

Die privaten Schlüssel werden innerhalb eines sicheren kryptografischen Devices (HSM) auf der geschützten Infrastruktur von Swisscom erzeugt. Für derart erstellte Zertifikate ist kein Verfahren zur Überprüfung des Besitzes des privaten Schlüssels nötig.

Falls die Antragsteller selbst im Besitz des privaten Schlüssels bleiben wollen, müssen sie einen mit dem zugehörigen privaten Schlüssel elektronisch signierten Zertifikatsantrag (CSR) stellen.

3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung

3.3.1 Zertifikaterneuerung

Sofern alle hinterlegten Dokumente für die Identifikation noch vorhanden sind und keine noch nicht überprüften Attribute oder Strukturen im neuen Zertifikat aufgenommen werden sollen, sind für eine Zertifikatserneuerung keine zusätzlichen Massnahmen zur Identifikation des Antragsstellers nötig. Bei der Beantragung der Erneuerung sind die dann gültigen Nutzungsbestimmungen der Swisscom zu akzeptieren. Voraussetzung für diese Art der Antragstellung ist, dass die Registrierungsstelle die Identität des Antragstellers innerhalb der letzten fünf 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 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:

- Persönliches Authentifizierungsmittel des Antragstellers.

Ungültigerklärung durch UID-Einheiten, die keine natürlichen Personen sind:

- Persönliche Mobiltelefonnummer einer der Vertreter der Antragstellerin, oder
- Von der Antragstellerin bereitgestelltes SSL/TLS-Client-Zertifikat als berechtigtes Authentisierungsmittel als Methode für die Freigabe von Fernsignaturen.

Sollte der Zertifikatsinhaber sein Authentisierungsmittel verloren haben, kann er die Revokation auch durch Übersendung eines unterzeichneten Widerrufsantrags unter Angabe der Seriennummer des Zertifikates per Post einreichen (Anschrift siehe Kap. 1.5). Zur Verifikation der Identität wird der Zertifikatsinhaber während der Geschäftszeit über die Firmenzentrale zurückgerufen, die Revokation wird erst danach vorgenommen.

4 Betriebsanforderungen an den Zertifikats-Lebenszyklus

4.1 Zertifikatsantrag

Zertifikatsanträge können von natürlichen Personen oder UID-Einheiten 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 durch Swisscom weiterbearbeitet:

- Die Nutzung durch natürliche Personen wird unmittelbar nach Bestätigung der Registrierungsstelle freigeschaltet.
- Die Nutzung durch UID-Einheiten wird innerhalb von 10 Arbeitstagen nach Bestätigung der Registrierungsstelle freigeschaltet.

4.3 Zertifikatausstellung

4.3.1 Zertifikatsausstellung für natürliche Personen

Zertifikate und kryptografische Schlüssel für natürliche Personen werden unmittelbar vor der Nutzung in einer zugriffsgeschützten Umgebung der Swisscom erstellt und zur Signaturerstellung vorgehalten. Der Zertifikatsinhaber kann Signaturen der beantragten Zertifikatsklasse durch Bestätigung auf dem bei der Identifikation registrierten Authentifizierungsmittel einsetzen (Signaturerstellungsdaten).

4.3.2 Zertifikatsausstellung für UID-Einheiten

Die Zertifikatausstellung läuft folgendermassen ab:

- Es wird sichergestellt, dass ein HSM eingesetzt wird,
- von Swisscom wird ein Zertifikat der gewünschten Klasse ausgestellt,
- das Zertifikat und der zugehörige kryptografische Schlüssel werden entweder
  - im Trust Center hinterlegt und das bei der Identifikation eingelieferte SSL/TLS-Client-Zertifikat wird mit dem zugehörigen Benutzerkonto verknüpft, so dass ausschliesslich durch den Besitz des zugehörigen privaten Schlüssels die Erstellung von Siegeln mittels Fernzugriff möglich ist (Signaturerstellungsdaten) oder
  - beim Kunden im HSM aufbewahrt, nachdem Swisscom sich versichert hat, dass der Kunde die erforderlichen Vorgaben einhält,
- die Zertifikatsinhaberin wird über die Bereitstellung informiert.

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 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 mit eigenem HSM versichert zudem, dass

- ein angemessenes Verständnis der Anwendung und des Einsatzes von Zertifikaten besteht,
- der private Schlüssel geschützt aufbewahrt wird,
- keiner unbefugten Person Zugang zu dem privaten Schlüssel gewährt wird,
- er unverzüglich auf das Erstellen weiterer Signaturen 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 Schlüsseln und Zertifikaten durch Zertifikatprüfer

Jede Person, die als Relying Party im Sinn von Kapitel 1.3 eine elektronische Signatur prüft, die auf einem Zertifikat gemäss dieser CP/CPS basiert, muss

- ein grundlegendes Verständnis der Anwendung und des Einsatzes von Zertifikaten besitzen;
- geeignete Komponenten und Verfahren zur Signaturprüfung einsetzen;
- die entsprechende Sperrliste (CRL) oder OCSP-Antwort überprüfen, bevor sie sich auf die Informationen 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, der private Schlüssel nicht kompromittiert wurde und die Algorithmen noch sicher sind. Zur Unterscheidung vom ursprünglichen Zertifikat muss das erneuerte Zertifikate eine unterschiedliche Seriennummer erhalten.

Die Identifikation des Zertifikatsinhabers muss den Anforderungen aus Kapitel 3.3.1 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 3.3 ein 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 Schlüssel oder sonstige Signaturerstellungsdaten zur Erstellung von Signaturen oder Siegel verloren, gestohlen, offengelegt 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 müssen 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 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;
  - das Zertifikat nicht oder nicht mehr den Vorgaben der zugrundeliegenden CP/CPS entspricht;
  - Swisscom Änderungen bekannt werden, die sich auf die Gültigkeit des Zertifikats auswirken;
  - der verwendete Krypto-Algorithmus oder die Schlüssellängen nicht mehr als sicher eingestuft werden;
  - einer der Gründe für Ungültigkeitserklärung durch den Zertifikatsinhaber vorliegt.

Die Gründe für die Revokation werden nicht ohne Einwilligung der Zertifikatsinhaber publiziert.

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 gemäss folgendem Prozess widerrufen:

- Der Zertifikatsinhaber richtet den Antrag für die Ungültigerklärung an die Registrierungsstelle, die den Identifikationsprozess durchführte.
- Die Registrierungsstelle bestätigt unverzüglich den Eingang des Antrags.
- Die Registrierungsstelle überprüft die Identität des Antragstellers gemäss Kapitel 3.4 und entscheidet innerhalb von 24 Stunden über den Antrag und die Publikation der Revokation.
- Wird festgestellt, dass ein gültiger Grund für die Ungültigerklärung vorliegt, wird das Zertifikat durch Swisscom innerhalb von 72 Stunden nach Erhalt des Antrags 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.

Weitere Fristen sind in Kapitel 4.9.4 definiert.

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.

Zertifikate der Klasse Diamant, die einmal in die CRL aufgenommen wurden, werden nicht mehr aus der CRL entfernt.

4.9.7 Suspendierung

Swisscom nimmt keine Suspendierung (zeitliche Aussetzung) von Zertifikaten oder Sperrung von kryptographischen Schlüsseln 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) an.

Swisscom stellt sicher, dass keine Kopien von Signaturschlüsseln erstellt werden und dass die privaten Signaturschlüssel nicht aus den HSM exportiert werden können.

Bei der Verwendung eines HSM kann mit speziellen Verfahren des HSM-Herstellers ein Backup hergestellt werden, das wiederum nur von einem definierten HSM wieder eingelesen werden kann.

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.

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 einer regelmässigen Überprüfung unterliegen. Solche Personen können Swisscom Mitarbeiter oder Vertragspartner sein. Sie haben Zugriff auf die Systeme der Swisscom PKI und führen 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. Die Zuweisung von vertrauenswürdigen Rollen an Personen wird jährlich überprüft.

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 Fachwissens, 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 allen Mitarbeitern mit Zugriff auf die Swisscom PKI 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 Sicherheits-technik 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 (inklusive dazugehörige Belege)
- Anträge auf Ungültigerklärung
- sämtliche Ereignisse, die den Lebenszyklus der von Swisscom verwalteten bzw. ausgestellten 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 beträgt im Zusammenhang mit Zertifikaten der Klasse "Diamant" mindestens 11 Jahre nach Ablauf der Gültigkeit des Zertifikats, im Zusammenhang mit Zertifikaten der Klasse "Saphir" mindestens 7 Jahre nach Ablauf der Gültigkeit des Zertifikats.

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 oder einer TSU 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 Schlüssel signiert und publiziert.

Falls ein 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 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 Schlüsseln einer CA

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

1. Widerruf des betroffenen CA-Zertifikats sowie aller noch gültiger Zertifikate, die von dieser CA ausgestellt wurden
2. Unverzügliche Information aller betroffenen Zertifikatsinhaber
3. Widerruf weiterer CA-Zertifikate, für welche die gleichen Kompromittierungsgründe vorliegen
4. Information der zuständigen Anerkennungsstelle
5. Der Vorfall, dessen Auswirkungen und die Revokationsinformationen werden auf der Webseite (gemäss Kapitel 2.1) veröffentlicht
6. Widerruf weiterer CA-Zertifikate, für welche die gleichen Einsatzbedingungen und Schwachstellen vorliegen (z.B. Schlüssel, die sich in derselben kryptographischen Vorrichtung befinden oder unter denselben Rahmenbedingungen erzeugt wurden)

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:

1. Benachrichtigung der Anerkennungsstelle und der Akkreditierungsstelle, mindestens 30 Tage vor Einstellung des Betriebes;
2. Widerruf aller noch gültigen von der Einstellung betroffenen Zertifikate;
3. Übergabe der Zertifikatsdatenbank an einen anderen anerkannten ZDA oder das BAKOM;
4. Die Zertifikatsinhaber werden von der Einstellung der Tätigkeit sowie vom Widerruf, der Übernahme oder der Weiterführung unverzüglich verständigt;
5. Übergabe der endgültigen Certificate Revocation Lists (CRL), des Transaktionsjournals sowie Registrierungsinformationen an die von der Akkreditierungsstelle benannte Stelle;
6. Sichere Zerstörung aller privaten Schlüssel der betroffenen CA der Swisscom PKI.

Sollte für den privaten Schlüssel der Root CA einer der Revokationsgründe nach Kap. 4.9.2 vorliegen, werden Informationen gemäss Kapitel 2.2 öffentlich publiziert. Die Punkte 2 und 5 entfallen.

6 Technische Sicherheitsmassnahmen

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 und TSS CA 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.

Die Schlüsselpaare der Zertifikate vom Typ „Diamant“ und „Saphir“ werden ebenfalls in einem HSM erzeugt und entsprechend den Vorgaben aus [ETSI EN 319 411-2] aufbewahrt. Das HSM erfüllt die Anforderungen gemäss Prüfstufe EAL4+.

6.1.2 Übermittlung des privaten Schlüssels an den Zertifikatsinhaber

Schlüsselpaare für Zertifikate der Klassen „Diamant“ und "Saphir" werden ausschliesslich innerhalb eines HSM erzeugt und gemäss den Anforderungen des HSM zur Einhaltung der Vertrauensstufe EAL4+ verwaltet. Hält der Zertifikatsinhaber das Schlüsselpaar auf einem eigenen HSM, wird ihm das HSM bzw. das Zertifikat zur Nutzung mit dem Schlüsselpaar auf dem eigenen HSM auf geeignete Weise übergeben.

6.1.3 Auslieferung des öffentlichen CA-Schlüssels

Alle Teilnehmer der Swisscom PKI können die öffentlichen Signaturprüfschlüssel (public key) der Swisscom Root-CAs 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:

Root CA 2 (OID 2.16.756.1.83.2.1)

- RSA 4096 SHA-256 für den CA 2 Root-Key
- RSA 2048 SHA-256 für die CAs der nachfolgenden Stufe (Level 1) und die TSS CA
- RSA 2048 SHA-256 für Enduser Zertifikate und die Zertifikate der TSUs

Root CA 4 (OID 2.16.756.1.83.30.4.0)

- RSA 8192 SHA256WithRSAandMGF1für den CA 4 Root-Key
- RSA 4096 SHA256WithRSAandMGF1für die CAs der nachfolgenden Stufe (Level 1) und die TSS CA
- RSA 3072 SHA-256 für Enduser Zertifikate und die Zertifikate der TSUs

Weitere Details (wie z.B. Padding-Algorithmen und Verwendungsdauer) sind im [Addendum] Profile der Zertifikate, Widerrufslisten und Online Statusabfragen definiert.

Die folgenden Hash-Algorithmen werden im Bereich des Signierens unterstützt:

- SHA-256
- SHA-384
- SHA-512

Falls der Signing-Request einen anderen Hash-Algorithmus enthält, wird er zurückgewiesen.

6.1.5 Parameter der öffentlichen Schlüssel und Qualitätssicherung

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

Zusätzlich entsprechen die Parameter der Zertifikate der Klasse "Diamant" auch den Anforderungen aus der [TAV], Kap. 2.3.3 sowie aus [ETSI EN 319 411-2].

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 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 genügen den Anforderungen von Art. 6 [ZertES] und 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 Schlüssels

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

6.2.3 Hinterlegung privater Schlüssel

Private Schlüssel von Zertifikatsinhabern werden nicht hinterlegt.

6.2.4 Backup der privaten 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 Schlüssel

Private 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, Issuing CAs oder Zertifikatsinhabern werden ausschliesslich in HSMs erstellt und gemäss den Anforderungen des HSM zur Einhaltung der Vertrauensstufe EAL4+ verwaltet.

6.2.7 Aktivierung der privaten Schlüssel

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

Bei fortgeschrittenen und qualifizierten Signaturen und fortgeschrittenen und geregelten Siegeln erfolgt die Aktivierung des privaten Schlüssels unter Angabe der von Swisscom bei der Identifikation (Kapitel 3.2) registrierten Signaturerstellungsdaten.

6.2.8 Deaktivierung der privaten Schlüssel

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

Bei fortgeschrittenen und qualifizierten Signaturen werden die privaten Schlüssel durch Beendigung der Verbindung zwischen HSM und der Signatur Software deaktiviert.

Die privaten Schlüssel zur Benutzung für fortgeschrittene und geregelten Siegel werden durch Beendigung der Verbindung zwischen HSM und der Signatur Software deaktiviert.

6.2.9 Vernichtung der privaten Schlüssel

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

Die privaten Schlüssel zur Benutzung für fortgeschrittene und qualifizierte Signaturen werden nach Ablauf der Zertifikatsgültigkeit oder bei Widerruf automatisch gelöscht.

Die privaten Schlüssel zur Benutzung für fortgeschrittene und geregelte Siegel werden vernichtet, wenn das Zertifikat gelöscht wird (z.B. nach Kündigung oder nach Ablauf der Gültigkeitsdauer).

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 Schlüssel

Öffentliche 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 inkl. TSS CA maximal 10 Jahre
- Zertifikate der Klassen „Diamant“ und „Saphir“ sowie die Zertifikate der TSUs maximal 3 Jahre

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

6.4 Aktivierungsdaten

Bei Serversignaturen verbleiben die privaten Schlüssel der Zertifikatsinhaber im HSM im Trust Center. Der Zertifikatsinhaber autorisiert die Benutzung seines privaten Schlüssels über die bei Swisscom registrierten Aktivierungsdaten (z.B. Mobiltelefonnummer).

6.4.1 Aktivierungsdaten für Schlüssel von natürlichen Personen

Aktivierungsdaten zur Nutzung von privaten Schlüsseln müssen den Anforderungen von [DIN EN 419 241-1] mindestens der Stufe 1 (Sole Control Assurance Level 1) entsprechen.

Für private Schlüssel Zertifikate der Klasse "Diamant" müssen Aktivierungsdaten die Anforderungen der Stufe 2 (Sole Control Assurance Level 2) erfüllen.

6.4.2 Aktivierungsdaten für Schlüssel von UID-Einheiten

Die Passwörter zur Aktivierung von privaten Schlüsseln zur Benutzung für fortgeschrittene und geregelte elektronische Siegel gemäss Kapitel 6.2.7 müssen mindestens 6 Zeichen lang sein.

6.4.3 Aktivierungsdaten für CA Schlüssel

Die Aktivierung der Schlüssel einer CA 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

Alle bei der Swisscom PKI eingesetzten Computer, Proxies und andere Komponenten werden einer Risikoanalyse unterzogen und ihrem Gefährdungspotential entsprechend abgesichert. Für die CA und den Directory Service wird zusätzlich eine Change Auditing Software eingesetzt, die einen Hash-Wert über die Konfigurationsfiles legt und somit Veränderungen feststellt werden können.

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 von einer akkreditierten Anerkennungsstelle 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:

- Jährliche Audits (Konformitätsprüfung durch akkreditierte Anerkennungsstelle)
- Regelmässige Evaluierung und Weiterentwicklung des Sicherheitskonzepts (jährlich)
- 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 falls erforderlich 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. Die Zertifikatsprofile und CRLs entsprechen ausserdem den Vorgaben von [RFC 5280] und die OCSP-Abfragen den Vorgaben von [RFC 6960]. Sie sind im [Addendum] zu dieser CP/CPS detailliert beschrieben.

8 Konformitätsüberprüfung (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.
- Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, [ZertES]), Stand am 1. Januar 2020

- Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Verordnung über die elektronische Signatur, [VZertES]), Stand am 2. Oktober 2020
- Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate ([TAV]), Stand am 15. März 2022
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI);
  General Policy Requirements for Trust Service Providers (2021-05)
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;
  Part 1: General requirements (2021-05)
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;
  Part 2: Requirements for trust service providers issuing EU qualified certificates (2021-11)
- ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
  Part 1: Overview and common data structures (2021-05)
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
  Part 2: Certificate profile for certificates issued to natural persons (2020-04)
- ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
  Part 3: Certificate profile for certificates issued to legal persons (2020-04)
- ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
  Part 5: QCStatements (2020-04)
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (2016-03)
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles (2016-03)
- DIN EN 419 241-1:2018: Trustworthy Systems Supporting Server Signing
  Part 1: General System Security Requirements (SCAL1 und SCAL2)
- ETSI TS 119 431-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers;
  Part 1: TSP service components operating a remote QSCD / SCDev (2021-05)
- ETSI TS 119 461: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects (2021-07)

8.2 Zertifizierung

Die Einhaltung der in Kap. 8.1 aufgeführten Gesetze und Regularien durch Swisscom als anerkannte Anbieterin von Zertifizierungsdiensten mit geregelten und qualifizierten Zertifikaten wurde von einer akkreditierten Prüfstelle überprüft und zertifiziert.

Zertifizierungsdienste auf der Basis der fortgeschrittenen Zertifikate (Zertifikatsklasse Saphir) sind in der Schweiz gesetzlich nicht geregelt. Gleichwohl lässt Swisscom die Einhaltung der in Kap. 8.1 aufgeführten Regularien durch eine geeignete externe Konformitätsbewertungsstelle prüfen.

8.3 Intervall und Umstände der Überprüfung

Die Anerkennungsstelle überprüft Swisscom sowie Registrierungsstellen in regelmässigen Abständen sowie bei sicherheitsrelevanten Veränderungen der CP/CPS.

8.4 Überprüfte Bereiche

Die von einer Überprüfung betroffenen Bereiche werden jeweils durch die zuständige Anerkennungsstelle festgelegt. Für Risiken, die zwingend eine Überprüfung notwendig machen, können bestimmte Bereiche im Voraus festgelegt werden.

8.5 Mängelbeseitigung

Aufgedeckte Mängel werden in Abstimmung mit der Anerkennungsstelle und Swisscom bzw. der überprüften Registrierungsstelle umgehend 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 mit einer im Sinne des [VZertES] genügenden Deckung.

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 eines 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.

Insbesondere nimmt Swisscom auf Ersuchen von Gerichten oder anderen Behörden eine Analyse der auf ihren Zertifikaten beruhenden elektronischen Signaturen vor.

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.

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

Für Zertifizierungsdienste auf der Basis von geregelten und qualifizierten Zertifikaten (Zertifikatsklasse Diamant) richtet sich die Haftung von Swisscom nach Art. 17 [ZertES]. Das vorliegende Dokument unterrichtet Zertifikatsinhaber über Beschränkungen der Verwendung der Dienste und diese Beschränkungen ergeben sich für dritte Beteiligte aus dem Zertifikat. Swisscom haftet deshalb nicht für Schäden, die bei einer über diese Beschränkungen hinausgehenden Verwendung der Dienste entstanden sind.

Swisscom Zertifikate können eine monetäre Obergrenze der Transaktionen für das Zertifikat nach Art. 7 Abs. 3 Bst. d [ZertES] enthalten. Sofern die Signatur aufgrund eines Zertifikats mit monetärer Obergrenze erstellt wurde, haftet Swisscom nicht für Schäden, die sich aus der Nichtbeachtung oder Überschreitung dieser Nutzungsbeschränkungen ergeben.

Die Obergrenze wird in den entsprechenden Zertifikaten gemäss Vorgaben aus [ETSI EN 319 412-5] in einem spezifischen Zertifikatsfeld `QcEuLimitValue` aufgeführt [Addendum].

Sofern Zertifizierungsdienste auf der Basis von fortgeschrittenen Zertifikaten (Zertifikatsklasse Saphir) erbracht werden oder andere Bereiche als die Erbringung des Zertifizierungsdienstes betroffen sind (z.B. im Verhältnis zwischen Swisscom und RA-Partnern) richtet sich 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

Über die bei der Registrierung angegebenen Kontaktdaten (z.B. Mobiltelefonnummer) informiert Swisscom direkt oder über den RA-Partner die Zertifikatinhaber über das Inkrafttreten einer neuen Version der CP/CPS oder der Nutzungsbestimmungen, sofern die Gültigkeitsdauer des Zertifikats noch nicht abgelaufen ist.

9.8.5 Änderungen dieses Dokuments

Änderungen an dieser CP/CPS werden in Absprache mit der Anerkennungsstelle 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 zwischen 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 gibt es auch eine englische Übersetzung.