

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

Version: 3.7

Datum: 10. Oktober 2023

Swisscom IT Services Finance S.E. ("Swisscom ITSF")

Mariahilfer Strasse 123/3

A-1060 Wien

## Änderungskontrolle

Version	Datum	Ausführende Stelle	Bemerkungen/Art der Änderung
3.0	05.04.2017	Kerstin Wagner, H-P Waldegger; Stéphane Vaucher	Erstellung einer CP/CPS nach eIDAS-VO und den neuen ETSI-Standards.
3.0	24.05.2017	Governance Board	Freigabe
3.1	19.04.2018	Kerstin Wagner, H-P Waldegger	Nachführen der Aktualisierungsintervalle der CRL und von OSCP; Aktualisierung der PKI Hierarchie; Präzisierung der zugelassenen Dokumente und Verfahren zur Ausstellung qualifizierter Zertifikate; Beschreibung der Kommunikation bei Änderungen.
3.1	15.06.2018	Governance Board	Freigabe
3.2	16.10.2018	H-P Waldegger	Diverse Präzisierung nach Audit und Nachführen CA 4
3.2	19.11.2018	Governance Board	Freigabe
3.3		Kerstin Wagner H-P Waldegger	Ergänzungen zur Root CA 4 Hierarchie, Erweiterung auf zusätzliche Authentisierungsmittel und Pflicht der Registrierungsstellen ein Umsetzungskonzept vorzulegen
3.3	22.01.2020	QTSP Board	Freigabe
3.4	15.06.2020	H-P Waldegger	Haftungsbeschränkung Kap. 9.7.1 ergänzt
3.4	18.01.2021	QTSP Board	Freigabe
3.5	03.06.2021	Kerstin Wagner	Korrektur der OID für die Root CA 2, Standorte für Backup angepasst, neue Root CA 4 Hierarchie, Aktualisierung CRL und OCSP-Service, Aktualisierung und Ergänzung der Regularien
3.5	22.12.2021	QTSP Board	Freigabe
3.6	26.01.2023	Kerstin Wagner	Ausserbetriebnahme der Diamant CA 2 und Saphir CA 2; Aktualisierung und Ergänzung der Regularien, Anpassung der Stellvertreterregelung, neue Identifikationsmethode für Saphir (fortgeschritten).
3.6	08.02.2023	QTSP Board	Freigabe
3.7	05.07.2023	Kerstin Wagner	Korrektur Archivierungszeitraum für archivierte Daten, Kap. 5.5.2, Aktualisierung bez. der relevanten Standards und der Güte der eingesetzten HSM (insbesondere in Kap. 3.2.2)
3.7	10.10.2023	QTSP Board	Freigabe

**Referenzierte Dokumente**

[eIDAS-VO]	Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
[SVG]	Österreichisches Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz)
[SVV]	Österreichische Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung)
[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 EU]	Addendum zum CP/CPS: Profile der Zertifikate, Sperrlisten (CRL) und Online Statusabfragen (EU)
[NB]	Nutzungsbestimmungen
[Sicherheitskonzept]	Sicherheitskonzept SDCS
[Rollenkonzept]	Rollenkonzept SDCS

**Inhaltsverzeichnis**

<b>1</b>	<b>Einleitung</b>	<b>8</b>
1.1	Überblick	8
1.2	Identifikation des Dokuments	8
1.3	Beteiligte der PKI (nachfolgend "die Beteiligten")	9
1.3.1	Certificate Authorities (CA)	9
1.3.2	Registrierungsstellen – Registration Authorities (RA)	10
1.3.3	Zertifikatsinhaber (Subscribers)	10
1.3.4	Zertifikatprüfer (Relying Parties)	10
1.3.5	Weitere Teilnehmer	10
1.4	Nutzung der Zertifikate (Certificate Usage)	11
1.4.1	Zulässige Zertifikatnutzung	11
1.4.2	Untersagte Zertifikatnutzung	11
1.5	Verwaltung der CP/CPS	11
1.6	Schlüsselwörter und Begriffe	11
1.7	Abkürzungen	14
<b>2</b>	<b>Veröffentlichungen und Verantwortung für den Verzeichnisdienst</b>	<b>15</b>
2.1	Verzeichnisdienst	15
2.2	Veröffentlichung von Informationen	15
2.3	Aktualisierung der Informationen	15
2.4	Zugang zu den Informationsdiensten	15
<b>3</b>	<b>Identifizierung und Authentifizierung</b>	<b>15</b>
3.1	Namen	15
3.1.1	Für natürliche Personen obligatorische Namensfelder	16
3.1.2	Für juristische Personen obligatorische Namensfelder	17
3.1.3	Optionale Namenselemente	17
3.1.4	Test-Zertifikate	17
3.2	Identitätsüberprüfung bei Neuantrag	18
3.2.1	Identifikation bei Anträgen von natürlichen Personen	18
3.2.2	Identifikation bei Anträgen von juristischen Personen	19
3.2.3	Nicht überprüfte Informationen	20
3.2.4	Verfahren zur Überprüfung des Besitzes des privaten Schlüssels	20
3.3	Identifizierung und Authentifizierung bei einer Zertifikaterneuerung	20
3.3.1	Routinemässige Zertifikaterneuerung (re-key)	20
3.3.2	Zertifikaterneuerung nach einer Ungültigerklärung	21
3.4	Identifizierung und Authentifizierung bei einer Ungültigerklärung	21
<b>4</b>	<b>Betriebsanforderungen an den Zertifikats-Lebenszyklus</b>	<b>22</b>
4.1	Zertifikatsantrag	22
4.2	Bearbeitung von Zertifikatsanträgen	22
4.3	Zertifikatsausstellung	22
4.3.1	Zertifikatsausstellung für natürliche Personen	22
4.3.2	Zertifikatsausstellung für juristische Personen	22
4.4	Zertifikatakzeptanz	22
4.5	Verwendung des Schlüsselpaares und des Zertifikats	22
4.5.1	Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatinhaber	22
4.5.2	Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Zertifikatprüfer	23
4.6	Zertifikaterneuerung unter Verwendung des alten Schlüssels (Certificate Renewal)	23
4.7	Zertifikaterneuerung unter Verwendung eines neuen Schlüssels (Re-Key)	23
4.8	Änderung von Zertifikaten	23
4.9	Ungültigerklärung und Suspendierung von Zertifikaten	23
4.9.1	Keine Ungültigerklärung bei kurzer Gültigkeitsdauer	23
4.9.2	Gründe für eine Ungültigerklärung	24
4.9.3	Wer kann die Ungültigerklärung vornehmen	24

4.9.4	Ablauf einer Ungültigerklärung eines Zertifikats .....	24
4.9.5	Fristen.....	25
4.9.6	CRL.....	25
4.9.7	Suspendierung.....	25
4.10	Dienst zur Statusabfrage von Zertifikaten .....	25
4.11	Beendigung des Vertragsverhältnisses durch den Zertifikatinhaber .....	25
4.12	Schlüsselhinterlegung und -wiederherstellung.....	25
<b>5</b>	<b>Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen .....</b>	<b>26</b>
5.1	Infrastrukturelle Sicherheitsmassnahmen .....	26
5.1.1	Lage und Konstruktion .....	26
5.1.2	Zutrittskontrolle .....	26
5.1.3	Stromversorgung und Klimatisierung.....	26
5.1.4	Abwehr von Wasserschäden .....	26
5.1.5	Feuer .....	26
5.1.6	Datenträger .....	26
5.1.7	Abfallentsorgung .....	26
5.1.8	Externes Backup .....	26
5.2	Organisatorische Sicherheitsmassnahmen .....	26
5.2.1	Vertrauenswürdige Rollen .....	26
5.2.2	Anzahl erforderlicher Mitarbeiter pro Aufgabe .....	27
5.2.3	Identifizierung und Authentisierung der Rollen .....	27
5.2.4	Trennung von Aufgaben.....	27
5.3	Personelle Sicherheitsmassnahmen .....	27
5.3.1	Anforderungen an die Mitarbeiter .....	27
5.3.2	Sicherheitsüberprüfung der Mitarbeiter.....	28
5.3.3	Anforderungen an die Schulung.....	28
5.3.4	Sanktionen für unautorisierte Handlungen.....	28
5.3.5	Dokumente für die Mitarbeiter .....	28
5.4	Sicherheitsüberwachung.....	28
5.4.1	Überwachte Ereignisse.....	28
5.4.2	Schutz der Protokolldaten.....	28
5.5	Archivierung.....	28
5.5.1	Archivierte Daten .....	28
5.5.2	Aufbewahrungszeitraum für archivierte Daten .....	29
5.5.3	Schutz der Archive.....	29
5.6	Schlüsselwechsel.....	29
5.7	Kompromittierung und Wiederherstellung .....	29
5.7.1	Prozeduren bei Sicherheitsvorfällen und Kompromittierung .....	29
5.7.2	Wiederherstellung von IT-Systemen .....	29
5.7.3	Kompromittierung von privaten Schlüsseln einer CA .....	29
5.7.4	Betrieb nach einer Katastrophe .....	30
5.8	Einstellung des Betriebes .....	30
<b>6</b>	<b>Technische Sicherheitsmassnahmen .....</b>	<b>30</b>
6.1	Schlüsselerzeugung und Installation .....	30
6.1.1	Schlüsselerzeugung .....	30
6.1.2	Übermittlung des privaten Schlüssels an den Zertifikatsinhaber.....	30
6.1.3	Auslieferung des öffentlichen CA-Schlüssels.....	30
6.1.4	Algorithmen und Schlüssellängen .....	31
6.1.5	Parameter der öffentlichen Schlüssel und Qualitätssicherung .....	31
6.1.6	Verwendungszweck der Schlüssel und Beschränkungen .....	31
6.2	Schutz des privaten Schlüssels.....	31
6.2.1	Standard der kryptografischen Module .....	31
6.2.2	Teilung des privaten Schlüssels.....	31
6.2.3	Hinterlegung privater Schlüssel .....	31

6.2.4	Backup der privaten Schlüssel.....	32
6.2.5	Archivierung der privaten Schlüssel.....	32
6.2.6	Erstellung und Speicherung privater Schlüssel.....	32
6.2.7	Aktivierung der privaten Schlüssel.....	32
6.2.8	Deaktivierung der privaten Schlüssel.....	32
6.2.9	Vernichtung der privaten Schlüssel.....	32
6.2.10	Güte des kryptografischen Moduls.....	32
6.3	Weitere Aspekte des Schlüsselmanagements.....	32
6.3.1	Archivierung öffentlicher Schlüssel.....	32
6.3.2	Gültigkeit von Zertifikaten und Schlüsselpaaren.....	33
6.4	Aktivierungsdaten.....	33
6.4.1	Aktivierungsdaten für Schlüssel von natürlichen Personen.....	33
6.4.2	Aktivierungsdaten für Schlüssel von juristischen Personen.....	33
6.4.3	Aktivierungsdaten für CA Schlüssel.....	33
6.5	Sicherheitsmassnahmen für Devices.....	33
6.5.1	Spezifische Anforderungen an technische Sicherheitsmassnahmen.....	33
6.5.2	Güte /Qualität der Sicherheitsmassnahmen.....	34
6.6	Lebenszyklus der Sicherheitsmassnahmen.....	34
6.6.1	Softwareentwicklung.....	34
6.6.2	Sicherheitsmanagement.....	34
6.7	Sicherheitsmassnahmen für das Netzwerk.....	34
6.8	Zeitstempel.....	34
<b>7</b>	<b>Profile für Zertifikate, Sperrlisten (CRL) und Online-Statusabfragen.....</b>	<b>34</b>
<b>8</b>	<b>Konformitätsüberprüfung (Compliance Audit) und andere Assessments.....</b>	<b>34</b>
8.1	Konformität.....	34
8.2	Zertifizierung.....	35
8.3	Intervall und Umstände der Überprüfung.....	35
8.4	Überprüfte Bereiche.....	35
8.5	Mängelbeseitigung.....	36
<b>9</b>	<b>Rahmenbestimmungen.....</b>	<b>36</b>
9.1	Vergütung.....	36
9.2	Haftpflichtversicherung von Swisscom.....	36
9.3	Vertraulichkeit von Geschäftsinformationen.....	36
9.3.1	Vertraulich zu behandelnde Daten.....	36
9.3.2	Nicht vertraulich zu behandelnde Daten.....	36
9.3.3	Verantwortung für den Schutz vertraulicher Informationen.....	36
9.4	Schutz von Personendaten (Datenschutz).....	36
9.4.1	Allgemein.....	36
9.4.2	Verantwortlicher Umgang mit Personendaten.....	36
9.4.3	Offenlegung gegenüber Gerichten und anderen Behörden.....	37
9.4.4	Andere Umstände einer Weitergabe von Daten an Dritte.....	37
9.5	Urheberrechte.....	37
9.6	Gewährleistung.....	37
9.6.1	Gewährleistung von Swisscom ITSF.....	37
9.6.2	Gewährleistungen anderer Beteiligter.....	37
9.7	Haftung.....	38
9.7.1	Haftung von Swisscom ITSF.....	38
9.7.2	Haftung anderer Beteiligter.....	38
9.8	Inkrafttreten und Aufhebung.....	38
9.8.1	Inkrafttreten.....	38
9.8.2	Aufhebung.....	38
9.8.3	Konsequenzen der Aufhebung.....	38
9.8.4	Individuelle Benachrichtigungen und Kommunikation mit Zertifikatsinhabern.....	39
9.8.5	Änderungen dieses Dokuments.....	39

9.9	Konfliktbeilegung .....	39
9.10	Anwendbares Recht und Gerichtsstand.....	39
9.11	Einhaltung des anwendbaren Rechts.....	39
9.12	Sprache .....	39

## 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 IT Services Finance S.E. zur Ausgabe von Zertifikaten im Sinne der EU Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt [eIDAS-VO], des Österreichischen Bundesgesetzes über die elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen [SVG] und der zugehörigen Signatur- und Vertrauensdiensteverordnung [SVV].

Swisscom IT Services Finance S.E. (nachfolgend "Swisscom ITSF") betreibt als qualifizierter Vertrauensdiensteanbieter einen Vertrauensdienst für die Ausstellung von fortgeschrittenen und qualifizierten Zertifikaten zur Nutzung für fortgeschrittene und qualifizierte elektronische Signaturen und fortgeschrittene und qualifizierte elektronische Siegel sowie zur Ausstellung von qualifizierten Zeitstempeln.

Die vorliegende CP/CPS bezieht sich auf verschiedene Zertifikatsklassen, "Diamant" für 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 Schlüssellängen den Anforderungen der nächsten Jahre standhalten.

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

### 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 Vertrauensdiensteanbieter:

- [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 VDA 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 Klasse „Diamant“ (qualifiziert) und „Saphir“ (fortgeschritten)“

**Version:** 3.7

<b>Object Identifier:</b>	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
	2.16.756.1.83.100.4.1	Diamant EU CA der Generationen 4 und 4.1
	2.16.756.1.83.100.4.2	Saphir EU CA der Generationen 4 und 4.1

Falls Zertifikate zusätzliche Ziffern in der OID enthalten, verweist diese auf die für das Zertifikat gültige Versionsnummer dieses Dokuments.

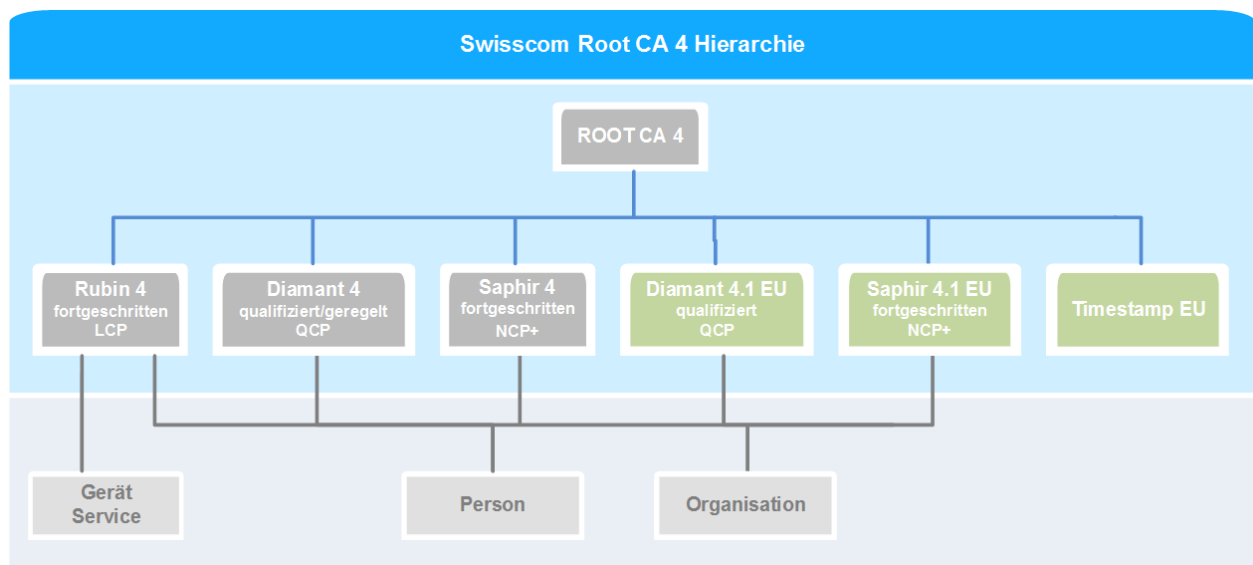
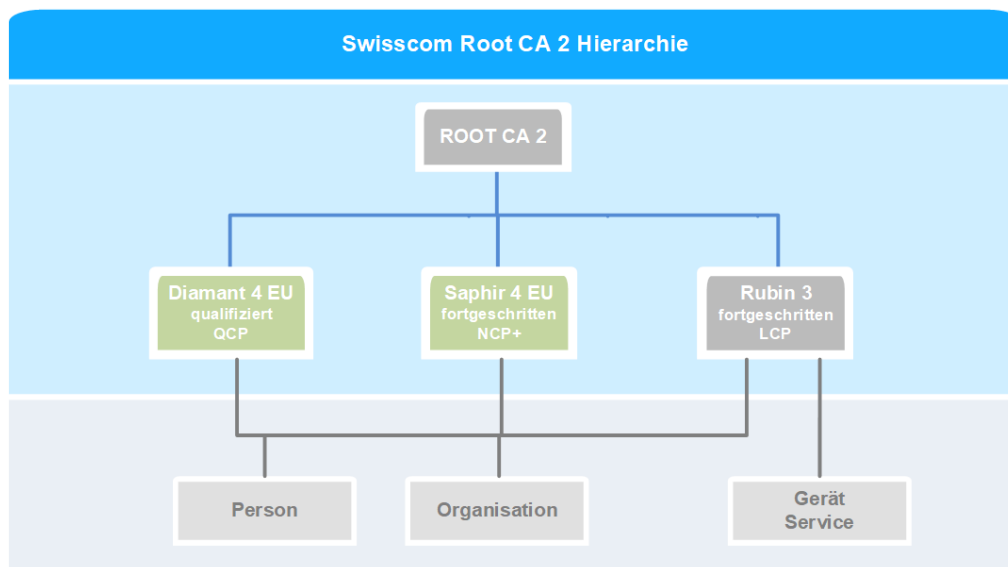
Die OID der Swisscom Digital Certificate Services basiert auf der vom schweizerischen Bundesamt für Kommunikation (BAKOM) zugeteilten RDN.



### 1.3 Beteiligte der PKI (nachfolgend "die Beteiligten")

#### 1.3.1 Certificate Authorities (CA)

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



Verantwortlich für die hier grün dargestellten und mit dem Zusatz "EU" bezeichneten CA ist Swisscom IT Services Finance S.E. mit Sitz in Wien. Diese CA richten sich nach der europäischen und österreichischen Gesetzgebung. Die grau dargestellten CA erfüllen die sehr ähnlichen Anforderungen aus der schweizerischen Gesetzgebung und sind Gegenstand einer eigenen Zertifikatsrichtlinie.

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

#### 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 ITSF aus.

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

#### **Diamant EU CA (qualifiziert)**

Zur Ausgabe von Zertifikaten der Klasse „Diamant“ für natürliche und juristische Personen. Entspricht den Definitionen für qualifizierte Zertifikate für elektronische Signaturen durch natürliche Personen von Art. 3 Z 15 [eIDAS-VO] und für elektronische Siegel für juristische Personen von Art. 3 Z 30 [eIDAS-VO] und verwendet ein sicheres kryptografisches Gerät (QSCD).

#### **Saphir EU CA (fortgeschritten – NCP+)**

Zur Ausgabe von Zertifikaten der Klasse „Saphir“ für natürliche und juristische Personen. Entspricht den Definitionen für elektronische Zertifikate zur Erstellung von fortgeschrittenen Signaturen durch natürliche Personen gemäss Art. 3 Z 11 [eIDAS-VO] und von Siegeln für juristische Personen von Art. 3 Z 26 [eIDAS-VO] und verwendet ein sicheres kryptografisches Gerät (QSCD).

#### **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. 3 Z 34 [eIDAS-VO]

### **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 ITSF kann die Aufgabe der Registrierung an Dritte (nachfolgend "RA-Partner") delegieren. RA-Partner werden mittels Vertrag verpflichtet, insbesondere die in diesem Dokument definierten Prozesse für die Registrierung, Zertifikatsausgabe, Revokation und Archivierung einzuhalten.

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 oder juristische Personen, die über den im Zertifikat definierten Namen eindeutig identifiziert werden können. Der Zertifikatsinhaber ist die Person, 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 oder juristische Personen, die die Zertifikate dieser PKI nutzen (z.B. Prüfung der Gültigkeit einer Signatur) und Zugang zu den Zertifizierungsdienstleistungen der Swisscom ITSF haben.

### **1.3.5 Weitere Teilnehmer**

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

## 1.4 Nutzung der Zertifikate (Certificate Usage)

### 1.4.1 Zulässige Zertifikatnutzung

Die Zertifikate dürfen nur für die Anwendungen benutzt werden, die in Übereinstimmung mit der im Zertifikat angegebenen Nutzung (keyUsage) stehen.<sup>1</sup>

Die im Rahmen dieser CP/CPS ausgestellten fortgeschrittenen Zertifikate "Saphir" können zum Erstellen von fortgeschrittenen elektronischen Signaturen oder fortgeschrittenen elektronischen Siegeln verwendet werden.

Die im Rahmen dieser CP/CPS ausgestellten qualifizierten Zertifikate "Diamant" können zum Erstellen von qualifizierten elektronischen Signaturen oder qualifizierten elektronischen Siegeln verwendet werden.

Die Schlüssel der Root-CA- werden ausschliesslich zum Signieren von CA-Zertifikaten und Sperrlisten verwendet.

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

### 1.4.2 Untersagte Zertifikatnutzung

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

Die Nutzung der Zertifikate zur Erstellung qualifizierter elektronischer Signaturen für Zertifikatsanträge nach eIDAS-VO Art 24 (1) c ist untersagt.

## 1.5 Verwaltung der CP/CPS

Herausgeberin dieses Dokuments ist:

Swisscom IT Services Finance S.E.  
 Swisscom Trust Services  
 Mariahilfer Strasse 123/3  
 A-1060 Wien

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

## 1.6 Schlüsselwörter und Begriffe

Begriff	Erklärung
Angaben zu den Zertifizierungspraktiken (CPS)	Angaben zu den Regeln und Richtlinien, die von vom VDA für die Ausstellung von Zertifikaten effektiv umgesetzt werden. Die CPS definiert die Ausrüstungen, die Methoden und die Verfahren, die von VDA in Übereinstimmung mit den von ihr gewählten Zertifikatsrichtlinien verwendet werden.
Aufsichtsstelle	Jeder Mitgliedstaat der EU ernennt eine Aufsichtsstelle, die die Aufsichtsaufgaben im benennenden Mitgliedstaat wahrnimmt, u.a. die Akkreditierung von Konformitätsbewertungsstellen (→ Bestätigungsstelle) und die Ausübung der Aufsicht über die in seinem Hoheitsgebiet niedergelassenen qualifizierten Vertrauensdiensteanbieter. In Österreich ist das Telekom-Control-Komitee (TKK) die Aufsichtsstelle für Vertrauensdiensteanbieter.

<sup>1</sup> Die farblich hervorgehobenen Rahmen werden nachfolgend verwendet, um Regelungen einer bestimmten Zertifikatsklasse – Orange für "Diamant" und Blau für "Saphir" zuzuordnen.

Begriff	Erklärung
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.
Bestätigungsstelle, Konformitätsbewertungsstelle	Von einer Aufsichtsstelle eines EU-Mitgliedstaates akkreditierte Stelle, die die Konformität qualifizierter Vertrauensdiensteanbieter und der von ihnen erbrachten qualifizierten Vertrauensdienste überprüft und zertifiziert.
Certificate Authority (CA), Issuing CA	Inстанz, 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
Digitales Zertifikat	elektronische Bescheinigung, die einen Signaturprüfchlüssel (private key) mit dem Namen einer Person, einer Organisation oder eines Systems verknüpft.
Elektronische Signatur	Technisches Verfahren zur Überprüfung der Echtheit eines Dokuments, einer elektronischen Nachricht oder der Identität des Absenders. Die elektronische Signatur und die handschriftliche Unterschrift werden bei Verwendung von digitalen Zertifikaten im Rahmen von Art. 4 [SVG] teilweise als gleichwertig betrachtet.
Generierung der Zertifikate	Dienst des VDA; 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.
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 (High 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 (Signator)	Natürliche und juristische Person, die Inhaberin des Signaturschlüssels ist, der dem im Zertifikat aufgeführten Signaturprüfchlüssel 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 VDA erzeugt und verwendet. Unmittelbar nach der Signaturerzeugung wird der private Schlüssel gelöscht.
qualifizierte elektronische Signatur	Die „qualifizierte elektronische Signatur“ ist eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht (Art. 3 Ziffer 12 [eIDAS-VO])
qualifiziertes elektronisches Siegel	Das „qualifizierte elektronische Siegel“ ist ein fortgeschrittenes elektronisches Siegel, die von einer qualifizierten elektronischen Siegelerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Siegel beruht (Art. 3 Ziffer 27 [eIDAS-VO])
QTSP (Qualified Trust Service Provider)	Geläufige englische Bezeichnung für qualifizierte Zertifizierungsdiensteanbieter (ZDA).
Qualifiziertes Zertifikat	digitales Zertifikat, das die Anforderungen aus Anhang I [eIDAS-VO] erfüllt.
RDN-Namen, Relative Distinguished Name	Namen der Verzeichniseinträge, deren Eindeutigkeit sich auf einen bestimmten Eintrag bezieht und die Bestandteile eines Verzeichnismens (Distinguished Name) sind.
Registrierung	Dienst der Registrierungsstelle, der darin besteht, die Identität und wenn nötig die Attribute jeder Antragstellerin und jedes Antragstellers eines Zertifikats zu überprüfen, bevor ihr/sein Zertifikat erzeugt oder die Aktivierungsdaten (oder das Passwort) zur Aktivierung der Nutzung des Signaturschlüssels zugewiesen werden.

Begriff	Erklärung
Schlüsselpaar	Signatur Schlüssel und dazugehöriger Signaturprüfschlüssel, die mathematisch durch einen asymmetrischen Signaturalgorithmus miteinander verknüpft sind.
Elektronische Signaturerstellungseinheit, elektronische Siegelerstellungseinheit	Für die Implementierung des Signatur Schlüssels konfigurierte Software/Firmware oder Hardware, den die Inhaberin oder der Inhaber des Zertifikats zur Erstellung einer elektronischen Signatur oder Siegels verwendet, z.B. eine SmartCard oder ein HSM.
Qualifizierte elektronische Signatur- oder Siegelerstellungseinheit	Signaturerstellungseinheit, die die Anforderungen aus Anhang II [eIDAS-VO] erfüllt.
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 VDA 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.
Signatur Schlüssel (private key)	Einmalige Daten wie Codes oder private kryptografische Schlüssel, die von der Inhaberin oder vom Inhaber zur Erstellung einer elektronischen Signatur oder Siegels verwendet werden.
Trust Center	Speziell geschützter Raum, in dem die Infrastruktur des VDA 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 gemäss [eIDAS-VO] und Schweizerischen Signaturgesetz angewendet werden.
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.
Vertrauensdiensteanbieter (VDA)	Eine Organisation, die digitale Zertifikate ausstellt und/oder andere Signatur- und Zertifizierungsdienste erbringt.
Ungültigerklärung des Zertifikats	Dienst des VDA, der die Gültigkeit eines Zertifikats vor dessen Ablauf aufhebt.
UTC, coordinated Universal Time	Universale Zeitskala auf Sekunden basierend. UTC ist definiert in der ITU-R Empfehlung TF.460-
Verteilung der Zertifikate	Dienst des VDA, 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 VDA, anhand dessen die Benutzerinnen und Benutzer eines Zertifikats überprüfen können, ob dieses für ungültig erklärt worden ist.
Zeitstempel	Dienst des VDA, der eine mit dem Datum, der Uhrzeit und einer qualifizierten Signatur versehene Bescheinigung abgibt, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt existiert haben.
Zeitstempel-Objekt Empfänger (Relying Party)	Empfänger eines Zeitstempel-Objektes, der diesem Zeitstempel-Objekt vertraut
Zeitstempel-Dienst Benutzer (Signator)	Natürliche Person, die eigene oder Daten einer juristischen Person oder Organisation durch einen Zeitstempel-Dienst zeitstempelt.
Zeitstempel-Objekt, Time-stamp 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.
Zeitstempel-Richtlinien (TP)	Spezifikation genereller Prozesse, die vom Zeitstempeldienst während des Erstellens von signierten Zeitstempeln verwendet werden.
Zeitstempel-Dienststelle (TSA)	Instanz, die Zeitstempel-Objekte erstellt.

Begriff	Erklärung
Zertifikatsrichtlinien (CP)	Gesamtheit von Regeln, welche die Anwendbarkeit eines Zertifikats für einen bestimmten Personenkreis und/oder eine Klasse spezieller Anwendungen mit gemeinsamen Sicherheitsanforderungen vorschreiben.

## 1.7 Abkürzungen

AIS	All-in Signing Service
BCP	Business Continuity Plan
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, erweitert um das Versicherungselement AVA_VAN.5 (Advanced methodical vulnerability analysis).
eIDAS-VO	Verordnung Nr. 910/2014 des europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
ISO	Information Security Officer, IT Sicherheitsverantwortlicher
LDAP	Lightweight Directory Access Protocol, Verzeichnisdienst
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol, Dienst zur Online Validierung von Zertifikaten
OID	Object Identifier
PDS	PKI Disclosure Statement
PED	PIN Entry Device
PIN	Personal Identification Number
QCP-l-qscd	Policy for EU qualified certificates issued to legal persons, where the private key and the related certificate reside on a QSCD
QCP-n-qscd	Policy for EU qualified certificates issued to natural persons, where the private key and the related certificate reside on a QSCD
QTSP	Qualified Trust Service Provider
RA	Registration Authority, Registrierungsstelle
Re-key	Zertifikaterneuerung mit neuen Schlüsseln
QSCD	Qualified electronic Signature/Seal Creation Device, sichere elektronische Signaturerstellungseinheit gemäss ISO/IEC 15408
QTSP	Qualified Trust Service Provider
SSL	Secure Socket Layer, Sicherheitsprotokoll
SVG	Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Signaturen (Signatur- und Vertrauensdienstegesetz –SVG)
SVV	Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Signaturen (Signatur- und Vertrauensdiensteverordnung –SVV)
TLS	Transport Layer Security
TSA	Time-stamping Authority
TSU	Time-stamping Unit
VDA	Vertrauensdiensteanbieter

## 2 Veröffentlichungen und Verantwortung für den Verzeichnisdienst

### 2.1 Verzeichnisdienst

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

Das Repository der Vertrauensdienste 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 der Root CAs
- Revokationsinformationen im Falle einer Kompromittierung der 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 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 Zertifikatsinhaber ist für solche Überprüfungen verantwortlich. Falls Swisscom ITSF bzw. die Registrierungsstelle über eine Verletzung solcher Rechte informiert wird, kann das Zertifikat von Swisscom ITSF 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 oder das vorgelegte Identifikations-Dokument des Zertifikatsinhabers ausgestellt wurde oder eine wirtschaftliche Beziehung (z.B. Bankkonto) unterhält.
Anzeigename	commonName (CN)	Informeller Name des Zertifikatsinhabers zur allgemeinen Darstellung.	Eine Darstellung des Namens, wie es der Zertifikatsinhaber oder der VDA zur benutzer- oder systemfreundlichen Darstellung für geeignet und verständlich hält.
Identität <i>entweder Vor- und Nachname</i>	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.
	<i>oder</i> 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: <ul style="list-style-type: none"> <li>• Von Swisscom vergebene Seriennummer</li> <li>• Von einer Registrierungsstelle vergebene Seriennummer mit einem spezifischen von Swisscom verwalteten Präfix</li> <li>• Zeichenfolge gemäss ETSI EN 319412-2 von "Natural person semantics identifier"</li> </ul> Bei Verwendung eines Pseudonyms, welches die Eineindeutigkeit sicherstellt, kann die serialNumber weggelassen werden.



### 3.1.2 Für juristische Personen obligatorische Namensfelder

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

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 das vorgelegte Identifikations-Dokument des Zertifikatsinhabers ausgestellt wurde oder eine wirtschaftliche Beziehung (z.B. Bankkonto) unterhält.
Anzeigename	commonName (CN)	Informeller Name des Zertifikatsinhabers zur allgemeinen Darstellung.	Eine Darstellung des Namens, wie es der Zertifikatsinhaber oder die VDA zur benutzer- oder systemfreundlichen Darstellung für geeignet und verständlich hält.
Identität	organization Name (O)	Formale Firma (Name des Unternehmers, unter dem er seine Geschäfte betreibt) des Zertifikatsinhabers	Exakte Wiedergabe des Inhalts des entsprechenden Feldes aus dem vorgelegten Identitätsdokument.
Eindeutigkeit	organization Identifier	Aus amtlicher Registernummer der Organisation abgeleitete Zeichenfolge	Zeichenfolge gemäss ETSI EN 319412-3 von "Legal person semantics identifier"

### 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.
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 nicht zugelassen.

### 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 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 Fernmeldediensteanbieters, der dem schweizerischen Fernmelderecht untersteht;
  - e. Die Angabe einer E-Mail Adresse, die im Zusammenhang mit den Zertifizierungsdiensten eingesetzt werden soll, unter folgenden Bedingungen:
    - i. Die E-Mail Domain wird von der Registrierungsstelle nur an Personen vergeben, deren Identität mittels amtlichen Lichtbildausweis geprüft wurde und die der Registrierungsstelle persönlich bekannt sind.
    - ii. Die Registrierungsstelle bestätigt den Besitz der Domain und kann diesen Besitz auf Anfrage nachweisen.
  - f. durch ein Zertifikat eines anerkannten Vertrauensdiensteanbieters 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 das Ablaufdatum der vorgelegten Dokumente, 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 ITSF.  
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 ITSF 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. 24 Abs. 1 [eIDAS-VO] von der Österreichischen Aufsichtsstelle zugelassen ist.
2. 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 ITSF genutzt werden.

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

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 (amtlicher Lichtbildausweis) gültig war.

### 3.2.2 Identifikation bei Anträgen von juristischen Personen

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

1. Der Vertreter des Antragstellers 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 des Antragstellers hat vorzulegen:
  - a. einen Auszug aus dem Firmenbuch oder einen aktuellen Auszug aus dem Register der Registrierungsagentur, die für das betreffende Land die Organisation registriert; Zulässig sind Register staatlicher Institutionen (Registergerichte, Bundeszentralamt für Steuern, berufsständischen Körperschaften öffentlichen Rechts oder vergleichbare) oder privatrechtliche Register (DUNS, vergleichbare Wirtschaftsdatenbanken, staatliche Institutionen des Privatrechts). Die Registereinträge werden nur dann als gültig akzeptiert, wenn Sie kein Attribut der Form "ungültig", "inaktiv" oder ähnliches enthalten. Nachweise werden hinterlegt.
  - b. sofern er nicht selbst im Firmenbuch oder einem anderen Register als alleine zeichnungsberechtigt eingetragen ist: eine Vollmacht zum Stellen eines Zertifikat-Antrags, ausgestellt vom geschäftsführenden Organ des Antragstellers (z.B. Vorstand oder Geschäftsführung) oder von im Register als zeichnungsberechtigt eingetragenen Personen.
  - c. Staatliche Einrichtungen/öffentlich-rechtliche Institutionen bestätigen zertifikatsrelevante Informationen mit Dienstsiegel und Unterschrift. Weiterhin können staatliche

Organisationen auf Grund gesetzlicher Legitimation authentisiert werden. Es kann vereinbart werden, dass die Nachweise bei der RA hinterlegt werden.

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

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

1. Der Vertreter des Antragstellers muss persönlich anwesend sein oder es muss ein Verfahren eingesetzt werden, dass in Österreich gemäss Art. 24 Abs. 1 [eIDAS-VO] zugelassen wurde.
2. Die Registrierung und Nutzung der Authentisierungsmittel muss mit einem vom Antragsteller 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 Identitätsnachweise und die Einwilligung zu den Nutzungsbestimmungen werden gemäss den Angaben in Kapitel 5.5.2 archiviert.

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.

## **3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung**

### **3.3.1 Routinemässige Zertifikaterneuerung (re-key)**

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 Zertifikaterneuerung keine zusätzlichen Massnahmen zur Identifikation des Antragstellers 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 Authentisierungsmittel des Antragstellers.

Ungültigerklärung durch juristische Personen.

- 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 Widerrufsanspruchs 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 oder juristischen Personen bei Registrierungsstellen der Swisscom ITSF (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 Zertifikatsantrag durch Swisscom ITSF weiterbearbeitet:

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

### **4.3 Zertifikatsausstellung**

#### **4.3.1 Zertifikatsausstellung für natürliche Personen**

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

#### **4.3.2 Zertifikatsausstellung für juristische Personen**

Die Zertifikatsausstellung läuft folgendermassen ab:

- Es wird sichergestellt, dass ein HSM eingesetzt wird,
- von Swisscom ITSF wird ein Zertifikat der gewünschten Klasse ausgestellt,
- das Zertifikat und der zugehörige kryptografische Schlüssel werden im Trust Center hinterlegt,
- das bei der Identifikation eingedielieferte 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 (Signaturstellungsdaten),
- der Zertifikatsinhaber wird über die Bereitstellung informiert.

### **4.4 Zertifikatakzeptanz**

Durch Verwendung des Zertifikats bzw. durch Freigabe der Signaturerstellung bei Fernsignaturen bestätigt der Zertifikatsinhaber bzw. Signator 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 Zertifikatsinhaber**

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

- sämtliche Angaben und Erklärungen des Zertifikatsinhabers in Bezug auf die im Zertifikat enthaltenen Informationen der Wahrheit entsprechen,
- die Signaturstellungsdaten (z.B. PIN oder Passwort) für die Freigabe der Signatur- bzw. Siegelstellung gemäss den Nutzungsbestimmungen der Swisscom ITSF 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 Schlüssels (Certificate Renewal)**

Swisscom ITSF erstellt keine neuen Zertifikate basierend auf einem bereits verwendeten Schlüssel (certificate renewal).

#### **4.7 Zertifikaterneuerung unter Verwendung eines neuen Schlüssels (Re-Key)**

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

Swisscom ITSF 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 Zertifikatsinhaber hat zu bestätigen, dass die bei der Identifikation (siehe Kapitel 3.2) aufgenommenen Informationen weiterhin gültig sind.

Es kommen die zum Zeitpunkt der Zertifikaterneuerung gültigen 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 ITSF für ungültig erklärt werden, wenn:

- der Zertifikatsinhaber (natürliche oder juristische Person) einen entsprechenden Antrag stellt oder
- Swisscom ITSF 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 ITSF ihre Tätigkeit ganz oder teilweise einstellt und ihre Verzeichnis- und Widerrufsdienste nicht von einem anderen VDA übernommen werden;
  - die Aufsichtsstelle gemäss Art. 6 SVG die Aussetzung des Zertifikats anordnet;
  - 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;
  - der verwendete Krypto-Algorithmus oder die Schlüssellängen nicht mehr als sicher eingestuft werden;
  - einer der Gründe für Ungültigkeitserklärung durch den Zertifikatsinhaber vorliegt.

#### 4.9.3 Wer kann die Ungültigerklärung vornehmen

Die folgenden Stellen können die Ungültigerklärung eines Zertifikats beantragen:

- Jeder Zertifikatnehmer kann von der Registrierungsstelle, die sein Zertifikat ausgestellt hat, verlangen, dass sein Zertifikat widerrufen wird;
- Swisscom ITSF kann jedes innerhalb der PKI ausgestellte Zertifikat nach eigenem Ermessen widerrufen;
- Eine Registrierungsstelle kann den Widerruf von Zertifikaten verlangen, deren Ausstellung sie beantragt hat;
- die Aufsichtsstelle kann den Widerruf eines Zertifikats anordnen.

#### 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. Die Fristen sind in Kapitel 4.9.5 beschrieben.

- Der Zertifikatsinhaber richtet den Antrag für die Ungültigerklärung an die Registrierungsstelle, die den Identifikationsprozess durchführte.
- Die Registrierungsstelle überprüft die Identität des Antragstellers und die Begründung für die Ungültigerklärung.



- Wird festgestellt, dass ein gültiger Grund für die Ungültigerklärung vorliegt, wird das Zertifikat durch Swisscom ITSF für ungültig erklärt.
- Swisscom ITSF aktualisiert die Sperrinformationen (OCSP) mit den ungültig erklärten Zertifikaten.
- Swisscom ITSF 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.

An Werktagen führen die Registrierungsstellen und Swisscom ITSF einen Antrag für eine Ungültigerklärung eines Zertifikats innerhalb von 3 Stunden nach Erhalt des Antrags aus. Ausserhalb dieser Zeit wird der Widerruf eines Zertifikats spätestens nach sechs Stunden nach Erhalt des Antrags ausgelöst.

#### **4.9.6 CRL**

Die CRL der Root CAs werden bei Bedarf, jedoch mindestens einmal im Jahr nachgeführt (Frequenz). Nach einer Veränderung wird eine neue CRL innerhalb von maximal 12 Stunden veröffentlicht (Latenz).

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

Die Statusinformationen sind mindestens 35 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 ITSF 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.

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

#### **4.11 Beendigung des Vertragsverhältnisses durch den Zertifikatinhaber**

Die Dauer des Vertragsverhältnisses ergibt sich aus der im Zertifikat angegebenen Zertifikats-Gültigkeitsdauer.

#### **4.12 Schlüsselhinterlegung und -wiederherstellung**

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

Swisscom ITSF 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 ITSF befinden sich in Trust Centern. Die wichtigen Komponenten sind redundant ausgelegt und befinden sich in zwei getrennten Rechenzentren von Swisscom (Schweiz) AG 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 berechnigte 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 unterbrechungsfreie Stromversorgung (no-break). Bei Stromausfällen wird Strom von einem Notstromaggregat produziert.

In den Trust Centern sorgen redundant ausgelegte Klimaanlage 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 ITSF Mitarbeiter oder Vertragspartner sein. Sie haben Zugriff

auf die Systeme der Swisscom PKI und führen Tätigkeiten 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 Mittel (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 (mit Aktualisierung alle drei Jahre):

- Strafregisterauszug
- Betreibungsregisterauszug.

### **5.3.3 Anforderungen an die Schulung**

In der Betriebsorganisation der Swisscom PKI werden ausschliesslich qualifizierte Mitarbeiter eingesetzt. Darüber hinaus werden regelmässige Schulungen für alle Mitarbeiter der Betriebsorganisation durch kompetente Personen durchgeführt.

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

Schulungen werden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und Sicherheitstechnik durchgeführt.

### **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 der 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 Aufbewahrungsfrist beträgt für Zertifikate der Klasse "Diamant" 30 Jahre und für Zertifikate der Klasse "Saphir" 7 Jahre nach Ablauf 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:

- Widerruf des betroffenen CA-Zertifikats sowie aller noch gültiger Zertifikate, die von dieser CA ausgestellt wurden
- Unverzügliche Information aller betroffenen Zertifikatsinhaber
- Widerruf weiterer CA-Zertifikate, für welche die gleichen Kompromittierungsgründe vorliegen
- Information der zuständigen Aufsichtsstelle
- Der Vorfall, dessen Auswirkungen und die Revokationsinformationen werden auf der Webseite (gemäss Kapitel 2.1) veröffentlicht
- 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:

- Benachrichtigung der Aufsichtsstelle, mindestens drei Wochen vor Einstellung des Betriebes;
- Legt die Aufsichtsstelle fest, dass der Widerruf der noch gültigen Zertifikate unzulässig ist, übergibt Swisscom dem Bund alle notwendigen Mittel und Informationen;
- Andernfalls Widerruf aller noch gültigen von der Einstellung betroffenen Zertifikate;
- Übergabe der Zertifikatsdatenbank an einen anderen qualifizierten VDA;
- Die Signatoren und Siegelersteller werden von der Einstellung der Tätigkeit sowie vom Widerruf, der Übernahme oder der Weiterführung unverzüglich verständigt;
- Übergabe der endgültigen Certificate Revocation List (CRL), des Transaktionsjournals und zugehöriger Belege an die von der Aufsichtsstelle benannte Stelle;
- Sichere Zerstörung aller privaten Schlüssel der betroffenen CA der Swisscom PKI.

### **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 Schlüsselpaare der Zertifikate vom Typ „Diamant“ und „Saphir“ werden ebenfalls in einem HSM erzeugt und aufbewahrt entsprechend den Vorgaben aus [ETSI EN 319 411-2]. Das HSM erfüllt die Anforderungen gemäss Prüfstufe EAL4+ bzw. FIPS 140-2 Level 3 oder höher. Die HSM sind so gelagert, dass bei der Schlüsselerzeugung das 4-Augen-Prinzip durch organisatorische Massnahmen erzwungen wird. Die Erstellung von CA-Schlüsseln wird dokumentiert.

##### **6.1.2 Übermittlung des privaten 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 einem eigenen HSM auf geeignete Weise übergeben.

##### **6.1.3 Auslieferung des öffentlichen CA-Schlüssels**

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

#### 6.1.4 Algorithmen und Schlüssellängen

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

Root CA 2 (OID 2.16.756.1.83.10)

- Mindestens RSA 4096 SHA-256 für den CA 2 Root-Key
- Mindestens RSA 2048 SHA-256 für die CAs der nachfolgenden Stufe (Level 1)
- Mindestens 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 SHA256WithRSAandMGF1 für den CA 4 Root-Key
- RSA 4096 SHA256WithRSAandMGF1 für 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. Algorithmen und Verwendungsdauer) sind im [Addendum EU] Profile der Zertifikate, Widerruflisten 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 [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 EU] zur 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 der [eIDAS-VO] und sind zertifiziert gemäss Prüfstufe EAL4+ bzw. FIPS 140-2 Level 3 oder höher.

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 Schlüsselpaaren 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**

Zur Aktivierung der privaten Schlüssel der CAs werden zwei verschiedene PED-keys, die im Besitz von 2 unterschiedlichen Schlüsselinhabern sind, verwendet. Damit wird das vier-Augen-Prinzip technisch sichergestellt.

Bei fortgeschrittenen und qualifizierten Signaturen und 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 qualifizierte 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 qualifizierte 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 TSU maximal 3 Jahre

Die Gültigkeitsdauer der Schlüssel und Zertifikate ist 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 der Klasse "Diamant" müssen Aktivierungsdaten die Anforderungen von [DIN EN 419 241-1] der Stufe 2 (Sole Control Assurance Level 2) erfüllen

#### 6.4.2 Aktivierungsdaten für Schlüssel von juristischen Personen

Die Passwörter zur Aktivierung von privaten Schlüsseln zur Benutzung für qualifizierte Siegel gemäss Kapitel 6.2.7 müssen mindestens 6 Zeichen lang sein. Nach 5-maliger Fehleingabe wird die PIN bzw. das Passwort gesperrt.

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

#### 6.4.3 Aktivierungsdaten für CA Schlüssel

Die Aktivierung der Schlüssel der CA im HSM erfordert die Beteiligung von mindestens zwei berechtigten Inhabern einer vertrauenswürdigen Rolle (gem. 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 feststellen 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 anerkannten Prüf- und Bestätigungsstellen 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:

- 2-jährliche Audits (Konformitätsprüfung durch anerkannten Prüf- und Bestätigungsstellen)
- 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 Zeitstempeldienst 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 EU] 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.
- Verordnung (EU) 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, in der Fassung vom 29.01.2015

- Österreichisches Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz, in der Fassung vom 1. Juli 2016)
- Österreichische Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung, in der Fassung vom 2. August 2016)
- 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 (2020-07)
- ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons (2020-07)
- 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 wurde durch die Telekom-Control-Kommission als Aufsichtsstelle im Rahmen der Konformitätsbewertung von Swisscom ITSF als qualifizierte Vertrauensdiensteanbieterin überprüft und zertifiziert.

## 8.3 Intervall und Umstände der Überprüfung

Swisscom ITSF beauftragt in regelmässigen Abständen von zwei Jahren sowie bei sicherheitsrelevanten Veränderungen der CP/CPS eine Konformitätsbewertungsstelle, die Einhaltung der Vorgaben gemäss diesen CP/CPS zu überprüfen. Darüber hinaus ist die Aufsichtsstelle gemäss Art. 20 Z 2 [eIDAS-VO] berechtigt, jederzeit stichprobenartige Überprüfungen der Swisscom ITSF (inklusive Registrierungsstellen) vorzunehmen.

## 8.4 Überprüfte Bereiche

Die von einer Überprüfung betroffenen Bereiche werden jeweils durch die zuständige Bestätigungsstelle 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 Aufsichtsstelle 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 der [eIDAS-VO] 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 ITSF trägt die Verantwortung für Massnahmen zum Schutz vertraulicher Informationen. Daten dürfen nur im Rahmen der Dienstleistung 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 ITSF weitergeben können und an die Swisscom ITSF 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 ITSF 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 ITSF zieht für die Erbringung der Vertrauensdienste Swisscom (Schweiz) AG mit Sitz in der Schweiz bei. Swisscom (Schweiz) AG betreibt die IT-Systeme zur Erbringung der Vertrauensdienste und diese Systeme stehen in der Schweiz. Die digitalen Zertifikate werden somit in der Schweiz ausgestellt. Es handelt sich deshalb um Auftragsdatenbearbeitung in der Schweiz durch Swisscom (Schweiz) AG, welche im Auftrag von Swisscom ITSF erfolgt. Einerseits hat Swisscom ITSF die hierfür erforderlichen datenschutzrechtlichen Vereinbarungen mit Swisscom (Schweiz) AG, andererseits willigen die Signatoren durch Annahme der Nutzungsbestimmungen hierzu ein.

### **9.4.2 Verantwortlicher Umgang mit Personendaten**

Swisscom ITSF und ihre RA-Partner halten sich 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 ITSF Auskunftspflichten 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 Signatoren 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 Signator im Zertifikat ein Pseudonym, hat Swisscom ITSF die Daten über die Identität des Signators zu übermitteln, sofern an der Feststellung der Identität ein überwiegendes berechtigtes Interesse im Sinne des § 8 Abs. 1 Z 4 und Abs. 3 DSG glaubhaft gemacht wird.

#### **9.5 Urheberrechte**

Swisscom ist Urheberin der folgenden Dokumente:

- vorliegende CP/CPS;
- dazugehörige Nutzungsbestimmungen.

Swisscom räumt den RA-Partnern und den Signatoren 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 ITSF**

Swisscom ITSF gewährleistet, dass die Angaben im Zertifikat den im Authentifikationsprozess gemäss diesem Dokument (Kapitel 3) gewonnenen Informationen entsprechen.

##### **9.6.2 Gewährleistungen anderer Beteiligter**

Weitere Gewährleistungen werden in den jeweiligen Verträgen mit Swisscom ITSF 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 ITSF

Für qualifizierte Vertrauensdienste richtet sich die Haftung von Swisscom ITSF nach Art. 13 [eIDAS-VO] und Art. 11 SVG. Das vorliegende Dokument unterrichtet Signatoren über Beschränkungen der Verwendung der Dienste und diese Beschränkungen ergeben sich für dritte Beteiligte aus dem Zertifikat und den genannten Haftungsbeschränkungen in den Nutzungsbestimmungen [NB]. Swisscom ITSF haftet deshalb nicht für Schäden, die bei einer über diese Beschränkungen hinausgehenden Verwendung der Dienste entstanden sind (Art. 13 Abs. 2 [eIDAS-VO]).

Swisscom Zertifikate können eine monetäre Obergrenze der Transaktionen für das Zertifikat enthalten. Sofern die Signatur aufgrund eines Zertifikats mit monetärer Obergrenze erstellt wurde, haftet Swisscom nicht für Schäden, die bei einer über diese Beschränkungen hinausgehenden Verwendung der Dienste entstanden sind.

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

Sofern nicht qualifizierte Vertrauensdienste betroffen sind (z.B. im Verhältnis zwischen Swisscom ITSF und RA-Partnern) richtet sich die Haftung von Swisscom ITSF nach den vertraglichen Vereinbarungen.

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

### 9.7.2 Haftung anderer Beteiligter

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

Die Haftung der RA-Partner ist Gegenstands des Vertrags zwischen Swisscom ITSF 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 von Swisscom (siehe Kapitel 2.2) veröffentlicht werden.

### 9.8.2 Aufhebung

Dieses Dokument ist gültig, bis:

- es durch eine neue Version ersetzt wird oder
- der Betrieb des Vertrauensdienstes von Swisscom ITSF 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 angegebene Kontaktdaten (z.B. Mobiltelefonnummer) informiert Swisscom ITSF direkt oder über den RA-Partner die Zertifikatsinhaber über das Inkrafttreten einer neuen Version der CP/CPS oder der Nutzungsbestimmungen, soweit die Gültigkeitsdauer des Zertifikats noch nicht abgelaufen ist.

#### **9.8.5 Änderungen dieses Dokuments**

Änderungen an dieser CP/CPS werden in Absprache mit der Bestätigungsstelle kommuniziert.

Die Kommunikation erfolgt gemäss Kapitel 9.8.4.

#### **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 ITSF gemäss diesem Dokument unterliegen der jeweiligen Regelung in den Verträgen (insbesondere Vertrag zwischen Swisscom ITSF und RA-Partner, Vertrag zwischen Swisscom ITSF und Zertifikatsinhaber).

Falls diese Verträge keine diesbezügliche Regelung enthalten, gilt:

- Unter Vorbehalt von anderslautendem zwingendem Recht (z.B. Konsumentenschutzbestimmungen), unterliegen alle Rechtsbeziehungen im Zusammenhang mit den Services von Swisscom ITSF gemäss diesem Dokument Österreichischem 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 Wien, Österreich.

#### **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.