Swisscom Digital Certificate Services

Certificate Policy (CP)

Zertifikatsklasse: „Saphir“ (fortgeschritten)

Übersicht	Certificate Policy für fortgeschrittene Zertifikate der Klasse „Saphir“ der Swisscom Digital Certificate Services.
Name	CP_Saphir_2_16_256_1_83
Version	2.7
Freigabe	10.10.2017
Ablauf	28.02.2018 (Ersatz durch CP/CPS_Diamant_Saphir_v3.0)
Klassifikation	public
OID	2.16.756.1.83.23.0 (Saphir CA 2)
Zugehöriges CPS	CPS Swisscom Digital Certificate Services OID: 2.16.756.1.83.2.1
Name der CA	Swisscom Saphir CA 2
OID der CA	2.16.756.1.83.23 (Saphir CA 2)
Inhaber der CA	Swisscom (Schweiz) AG
Sprache	Deutsch (rechtlich verbindliche Originalversion)
	English translations of selected sections in the Appendix (original version in German is legally binding)
Beginn der CP Konformitätsprüfung	01. Januar 2011 (Saphir CA 2)
Dokumenten Freigabe	Governance Board der Swisscom Digital Certificate Services

Änderungskontrolle

Version	Datum	Ausführende Stelle	Bemerkungen/Art der Änderung
2.0	04. 11.2011	Projektteam	Ergänzungen SHA-256, Unterscheidung CA 1 und CA 2
2.1	17.12.2012	Governance Board	Übersetzung in Englisch / Freigabe
2.2	28.01.2014	Projektteam	Erweiterungen für All-in Signing Service
2.3	17.07.2014	Kerstin Wagner	Review und Update
2.4	15.01.2015	Kerstin Wagner	Überarbeitung nach dem Review von *Legal & Compliance* (Swisscom)
2.5	14.08.2015	Kerstin Wagner	Anpassung Kapitel 3.1.1 Namensform, Ergänzung der Verfahren zur Identitätsüberprüfung, Kap. 3.2
2.6	28.04.2016	Kerstin Wagner	Auslagerung der Angaben zu den CAs der 1. Generation (CA 1) in ein eigenständiges Dokument; Review und Update 2016
2.7	12.09.2017	H-P Waldegger	Übergangsbestimmungen zur Ablösung dieses Dokuments durch die neue CP/CPS Version 3 auf Basis des revidierten ZertES [14].
2.7	10.10.2017	Governance Board	Freigabe

Referenzierte Dokumente:

[1] SR 943.03, ZertES: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur) vom 19. Dezember 2003 (Stand am 1. August 2008)

[2] SR 943.032, VZertES: Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (Verordnung über die elektronische Signatur) vom 3. Dezember 2004 (Stand am 1. August 2011)

[3] SR 943.032.1, Verordnung des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur, inklusive TAV-ZertES (Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur) vom 6. Dezember 2004 (Stand am 1. August 2011)

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

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

[6] CPS Swisscom Digital Certificate Services, OID 2.16.756.1.83.2.1

[7] Addendum zum CPS [6]: Profile der Zertifikate, Widerrufslisten (CRL) und Online Statusabfragen

[8] SR 641.201.511 Verordnung des EFD über elektronische Daten und Informationen (ElDI-V) vom 11. Dezember 2009 (Stand am 1. Januar 2010)

[9] SR 641.201.511.1, Verordnung der ESTV über Zertifizierungsdienste im Bereich der ElDI-V inklusive Anhang TAV-ElDI-V (Technische und administrative Vorschriften für Zertifizierungsdienste im Bereich der ElDI-V im Zusammenhang mit der Ausstellung von Zertifikaten basierend auf fortgeschrittenen Signaturen) vom 14. Dezember 2009 (Stand am 1. Januar 2010)

[10] SR 221.431 Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (Geschäftsbücherverordnung; GeBüV)

[11] ETSI TS 101 862: Technical Specification: Qualified Certificate profile

[12] 641.201.511, Verordnung des EFD über elektronische Daten und Informationen (ElDI-V) vom 11. Dezember 2009 (Stand am 1. Januar 2017)

[13] SR 943.03, ZertES: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (auch genannt: Bundesgesetz über die elektronische Signatur) vom 18. März 2016 (Stand am 1. Januar 2017)

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument beschreibt die Certificate Policy (Zertifizierungsrichtlinie, nachfolgend CP) von Swisscom Digital Certificate Services zur Ausgabe von digitalen Zertifikaten zur Erstellung von fortgeschrittenen elektronischen Signaturen gemäss Art. 2 Bst. b ZertES [1] sowie nach ElDI-V [8] inklusive den daraus abgeleiteten technischen und administrativen Ausführungsbestimmungen TAV–ElDI-V [9] und der Geschäftsbücherverordnung (GeBüV) [10].

Die CP erlaubt Benutzern und Dritten, welche dem Zertifikat vertrauen (Relying Parties), die Vertrauenswürdigkeit der durch Swisscom (Schweiz) AG (nachfolgend Swisscom) als Anbieterin von Zertifizierungsdiensten (nachfolgend Certification Service Provider, CSP) und ihren Registrierungs-Stellen (RA) ausgestellte Zertifikate abzuschätzen.

Ein „Saphir" Zertifikat ist eine elektronische Bescheinigung, mit der ein öffentlicher kryptografischer Schlüssel einer Person oder Organisation zugeordnet und mit der die Identität der Person oder Organisation bestätigt wird. Ein Zertifikat stellt also eine Verbindung zwischen einer Person oder Organisation und einem kryptografischen Schlüssel her.

Die Bezeichnung „fortgeschritten" in Bezug auf elektronische Signaturen ist in Art. 2 Bst. b ZertES folgendermassen umschrieben: eine *fortgeschrittene elektronische Signatur* ist eine elektronische Signatur, die folgende Anforderungen erfüllt:

- Sie ist ausschliesslich der Inhaberin oder dem Inhaber zugeordnet.
- Sie ermöglicht die Identifizierung der Inhaberin oder des Inhabers.
- Sie wird mit Mitteln erzeugt, welche die Inhaberin oder der Inhaber unter ihrer oder seiner alleinigen Kontrolle halten kann.
- Sie ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Jedes Zertifikat ist nur so vertrauenswürdig wie die Verfahren, nach denen es ausgestellt wird. Swisscom teilt dazu Zertifikate in „Zertifikatklassen" ein. Je höher die Zertifikatklasse, desto umfangreichere Identifikationsprüfungen liegen der Ausstellung eines Zertifikates zugrunde. Die Zertifikate selbst enthalten als Information die Angabe über die Klasse des Zertifikats. Die detaillierten Prozesse der Prüfungen, welche hinter einer Zertifikatklasse stehen sowie die allgemeinen Sicherheitsvorkehrungen können dem Certification Practice Statement (nachfolgend CPS [8]) der Swisscom Digital Certificate Services entnommen werden.

Diese CP bezieht sich auf die Zertifikatklasse „Saphir" und entspricht – bei Durchlaufen der Prozesse gemäss Kapitel 3.2.2 – den Anforderungen der eidgenössischen Steuerverwaltung über elektronische Daten und Informationen (ElDI-V [8]). Für alle Zertifikate, die dieser CP entsprechen, ist der Objekt Bezeichner gemäss X.509 [OID] dieser CP im Zertifikat vermerkt. Somit wird die CP an das Zertifikat einer bestimmten Zertifikatsklasse gebunden.

Die Zertifikatsklasse „Saphir" entspricht der Definition gemäss Art. 2 Bst. b ZertES [1] für fortgeschrittene Zertifikate und verwendet zusätzlich eine sichere Signaturerstellungseinheit (nachfolgend SSCD genannt; entsprechend den im CPS [5], Kapitel 3.2.1, beschriebenen Verfahren). Die fortgeschrittene elektronische Signatur ist der handschriftlichen Unterschrift nicht gleichgestellt, ist aber geeignet, die Identität (Authentizität) einer Person oder Organisation nachzuweisen und die signierten Dokumente vor Veränderungen zu schützen. Diese Zertifikatsklasse wird für natürliche Personen und Organisationen ausgestellt und kann zum Signieren von Daten aller Art und zum Authentisieren verwendet werden.

Swisscom stellt sicher, dass die Saphir Zertifikate in der selben Infrastruktur und mit den selben Prozessen betrieben werden wie die Zertifikatsklasse „Diamant“ (qualifiziert), welche die Vorgaben des ZertES [1], der zugehörigen Verordnung (VZertES [2]) und der daraus abgeleiteten technischen und administrativen Vorschriften (TAV-ZertES [3]) erfüllen. Die Einhaltung dieser Vorgaben wird durch eine von der Schweizerischen Akkreditierungsstelle (SAS) akkreditierte Anerkennungsstelle geprüft.

1.1 Überblick

Diese CP wurde von Swisscom zu folgendem Zweck erstellt:

- Erfüllung der Anforderungen an einen Certificate Service Provider (nachfolgend CSP) von digitalen Zertifikaten zur Erstellung fortgeschrittene elektronischer Signaturen gemäss ZertES [1].
- Erfüllung der Anforderungen an einen CSP von digitalen Zertifikaten zur Erstellung fortgeschrittener elektronischer Signaturen gemäss ElDI-V [8] und GeBüV [10]
- Beschreibung der Dienstleistungen, Rollen, Einschränkungen und Verpflichtungen bei der Verwendung von Zertifikaten der Zertifikatsklasse „Saphir“ der Swisscom.
- Sicherstellung der Interoperabilität bei der Benutzung fortgeschrittener Zertifikate der Swisscom.

Die Struktur der CP orientiert sich an den Vorgaben des RFC 3647 [4]. Das Framework CP und CPS wurde nach den Vorgaben für einen Dienstanbieter zur Aufgabe von qualifizierten Zertifikaten nach folgenden Standards aufgesetzt:

- TAV (SR 943.032.1) [3]
- ETSI TS 101 456 [5]
- ETSI TS 101 862 [11]

Um die internationale Zusammenarbeit mit anderen Zertifizierungsstellen zu ermöglichen, werden ferner gewisse Kapitel dieser CP ins Englische übersetzt (siehe Anhang); massgeblich ist in jedem Fall die deutsche Version in der jeweils aktuellen Fassung.

1.2 Identifikation des Dokuments

Identifikation

- Titel: Swisscom Digital Certificate Services - Certificate Policy (CP) für die Zertifikatsklasse „Saphir“
- Version: 2.7
- Object Identifier (OID) für diese CP: 2.16.756.1.83.23.0

Die OID der Swisscom Digital Certificate Services basiert auf der vom BAKOM zugeteilten RDN:

1. Stelle	2. Stelle	3. Stelle	4. Stelle	5. Stelle	Bedeutung
2					Joint ISO-CCITT Tree
	16				Country
		756			Switzerland
			1		Organisation Names (RDN)
				83	Swisscom Digital Certificate Services

Die Stellen 6 bis 8 der OID von Swisscom Digital Certificate Services verweisen auf die jeweilige CA bzw. auf das jeweilige CP/CPS Dokument.

Die vom BAKOM vergebenen OID können auf der Internetseite des BAKOM abgefragt werden (http://www.eofcom.admin.ch/eofcom/public/searchEofcom_oid.do).

1.3 Beteiligte der Swisscom Digital Certificate Services

1.3.1 Certification Authorities

Als anerkannte Anbieterin von Zertifizierungsdiensten betreibt Swisscom eine offline Root Certification Authority (nachfolgend CA) sowie eine der Root CA untergeordnete CA für fortgeschrittene Zertifikate der Klasse „Saphir“. Die Swisscom Root CA ist an keinem Netzwerk angeschlossen und wird nur dann gestartet, wenn dies erforderlich ist. Die Root-CA stellt ausschliesslich Zertifikate für unmittelbar nachgelagerte CAs der Swisscom Digital Certificate Services aus.

Für den Betrieb der CA und die Funktionstrennung gelten die Vorgaben der TAV-ZertES [3].

1.3.2 Registrierungsstellen – Registration Authorities (RA)

Die Registrierungsstellen sind im Kapitel 1.3.2 der zugehörigen CPS [6] beschrieben.

1.3.3 Zertifikatinhaber (Subscriber)

Ein „Saphir“ Zertifikat kann auf eine natürliche oder eine juristische Person sowie auf weitere definierte Organisationen ausgestellt werden.

Nur durch die RA registrierte Personen können Mutationen, Updates und eine Ungültigerklärung des Zertifikates veranlassen. Verlässt ein für ein Zertifikat registrierter Zertifikatsinhaber während der Gültigkeitsdauer des Zertifikates eine juristische Person oder zieht die juristische Person die

Vollmacht zur Vertretung der juristischen Person zurück, muss sich ein Nachfolger bei der RA registrieren. Zu jedem Zeitpunkt der Zertifikatsgültigkeit muss eine natürliche Person als bevollmächtigter Zertifikatsinhaber bei der RA registriert sein.

1.3.4 Zertifikatprüfer (Relying Parties)

Die Zertifikatprüfer sind im Kapitel 1.3.4 der zugehörigen CPS [6] beschrieben.

1.3.5 Weitere Teilnehmer

Die weiteren Teilnehmer sind im Kapitel 1.3.5 der zugehörigen CPS [6] beschrieben.

1.4 Anwendbarkeit der Zertifikate (Certificate Usage)

1.4.1 Geeignete Zertifikatnutzung

Die im Rahmen dieser CP ausgestellten Zertifikate können durch den Zertifikatinhaber für die elektronische Signatur und die Authentisierung verwendet werden. Eingeschlossen ist bei Durchlaufen der Prozesse gemäss Kapitel 3.2.2 die Verwendung für ElDI-V [10] konforme Signaturen.

Die Zertifikatinhaber sind selbst für die Benutzung der Zertifikate in den Anwendungsprogrammen zuständig. Für eine gültige fortgeschrittene Signatur müssen die Verfahren und Mittel verwendet werden, die durch Swisscom definiert werden. Die verwendeten Anwendungsprogramme müssen dazu den Sicherheitsanforderungen geeignet Rechnung tragen. Eine Installation von Anwendungsprogrammen durch Swisscom sowie durch deren Vertragspartner findet nicht statt.

1.4.2 Untersagte Zertifikatnutzung

Die Zertifikatsnutzung ausserhalb des in den Nutzungsbestimmungen definierten Anwendungsbereichs ist untersagt.

1.5 Verwaltung der Richtlinien

Herausgeberin des Dokumentenframeworks ist:

Swisscom (Schweiz) AG
Digital Certificate Services
Postfach
8021 Zürich

Es gilt ein formelles Genehmigungsverfahren gemäss CPS [6], Kapitel 9.11.

1.6 Schlüsselwörter und Begriffe

Schlüsselwörter und Begriffe sind Abschnitt 1.6 der CPS [6] zu entnehmen.

1.7 Abkürzungen

CA	Certification Authority
CN	Common Name, als Teil des DN gemäss RFC 3739
CP	Certificate Policy, Zertifizierungssrichtlinien
CPS	Certification Practice Statement, Angaben zum Zertifizierungsbetrieb
CSP	Certificate Service Provider, Anbieter von Zertifizierungsdiensten
CRL	Certificate Revocation List
DN	Distinguished Name gemäss RFC 3739
EFD	Eidgenössisches Finanz Departement
ElDI-V	Verordnung des EFD über elektronische Daten und Informationen
ESTV	Eidgenössische Steuerverwaltung
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
ISO	Information Security Officer, IT Sicherheitsverantwortlicher
LDAP	Lightweight Directory Access Protocol, Verzeichnisdienst
E-RA	Local Registration Authority / Lokale Registrierungsstelle bei einem RA Partner
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OeIDI	Ordinance of the FDF on Electronic Data and Information (zu Deutsch: ElDI-V)
PED	PIN Entry Device
PIN	Personal Identification Number, Persönliche Nummer zum Aktivieren des Signaturschlüssels
RA	Registration Authority / Registrierungsstelle (umfasst RA der Swisscom und RA/TPS)
Re-Key	Zertifikaterneuerung
SSCD	Secure Signature Creation Device (Sichere Signaturerstellungseinheit) gemäss ETSI TS 101 456. Swisscom setzt HSM und SmartCards als SSCD ein.
SSL	Secure Socket Layer, Sicherheitsprotokoll
TSP	Time Stamping Profile
TPS	Trusted Point of Sales
TSA	Time-Stamping Authority
TAV-ElDI-V	Technische und administrative Vorschriften für Zertifizierungsdienste im Bereich der ElDI-V im Zusammenhang mit der Ausstellung von Zertifikaten basierend auf fortgeschrittenen Signaturen
TAV-ZertES	Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur

2 Veröffentlichungen und Verantwortung für den Verzeichnisdienst

Details sind dem CPS [6], Kapitel 2, zu entnehmen.

3 Identifizierung und Authentifizierung

3.1 Namen

3.1.1 Namensform

Alle innerhalb der Swisscom Digital Certificate Services ausgestellten Zertifikate beinhalten eindeutige Namen (Distinguished Name, nachfolgend DN) entsprechend der Normenserie X.500. Ein DN enthält eine Folge von obligatorischen und optionalen Namensattributen, durch die alle Teilnehmer einer Hierarchie eindeutig referenziert werden können.

Folgende Daten und Nachweise müssen erfasst werden:

Saphir (fortgeschritten)	**Namenselement (DN)**	**Erforderlicher Nachweis**
Obligatorisch	CN = <Titel, Vorname, Mittelname, Name *oder* Name der Organisation *oder* Pseudonym>	Gemäss Kapitel 3.2.3 Gemäss Kapitel 3.2.2 Gemäss Kapitel 3.1.3
	C = <ISO-Ländercode, zweistellig>	Ländercode des Landes, in dem das vorgelegte Identifikationsdokument des Zertifikatsinhabers ausgestellt wurde (bei natürlichen Person) oder die Organisation registriert ist (bei juristischen Personen).
Optional	<serialNumber>	Falls erforderlich, z.B. bei Namensgleichheit: zusätzliche Nummer, die die Eindeutigkeit des DN sicherstellt.
	SN = <Nachname> GN = <Vorname> O = <Organisation> OU = <Organisationseinheit> L = <Ortschaft> ST = <Kanton> STREET = <Postanschrift> E = <Email-Adresse> pseudonym = <Pseudonym> organizationIdentifier = <aus Unternehmens-Identifikationsnummer nach UIDG abgeleitete Zeichenfolge>	Gemäss Kapitel 3.2.2 bzw. 3.2.3

Für alle im DN erfassten Attribute müssen Nachweise erbracht werden. Eine Organisationsbezeichnung (O=) wird nur eingetragen, wenn die Anforderungen gemäss Kapitel 3.2.2 erfüllt werden.

Die Einzelheiten der Attribute sind im CPS [6] Kapitel 3.1.1 festgelegt.

3.1.2 Aussagekraft von Namen

Bei der Vergabe des DN gelten grundsätzlich die folgenden Regelungen:

- Der DN muss den Zertifikatinhaber eindeutig identifizieren und in einer für Menschen verständlichen Form vorliegen.
- Zertifikate dürfen nur auf einen zulässigen, in amtlichen Dokumenten vermerkten Namen des Zertifikatinhabers ausgestellt werden.
- Soll der Name der natürlichen Person, welche den Signaturschlüssel kontrolliert, nicht im Zertifikat enthalten sein, muss der DN als Pseudonym gekennzeichnet sein. Dies trifft auch auf Firmen- und Organisationszertifikate zu.
- Bei der Vergabe des DN für Firmen- oder Organisationszertifikate muss eine Verwechslung mit natürlichen und juristischen Personen oder Bezeichnungen von Organisationseinheiten ausgeschlossen werden. Ebenso dürfen keine DNS-Namen, IP-Adressen oder andere innerhalb der Swisscom Digital Certificate Services benutzte Syntaxelemente verwendet werden. Ein Pseudonym darf keinen beleidigenden oder anzüglichen Inhalt enthalten oder gegen Rechtsnormen oder Rechte Dritter (v.a. Namensrecht) verstossen.
- Diskriminierungen in jeglicher Form sind unzulässig.

Darüber hinaus wird jedem Zertifikat eine eindeutige Zertifikats-Seriennummer zugeordnet, welche eine eindeutige und unveränderliche Zuordnung zum Zertifikatinhaber ermöglicht. Die Einzelheiten sind im CPS [6] Kapitel 3.1.2 festgelegt.

3.1.3 Pseudonymität / Anonymität

In begründeten Ausnahmen und sofern das Zertifikat nicht für ElDI-V [8] - Zwecke eingesetzt werden soll, kann für eine natürliche Person anstelle des Namens im Zertifikat ein Pseudonym bzw. eine eindeutige Anonymisierung aufgeführt werden. Dieses wird im CN-Feld des DN eindeutig kenntlich gemacht. Für die Eindeutigkeit von Pseudonymen gelten weiterhin auch die Regelungen unter 3.1.5.

Die Identitätsprüfung erfolgt immer entsprechend den Regelungen unter Kapitel 3.2. Anonyme Zertifikate sind daher nicht möglich.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Der zu verwendende Zeichensatz und die Substitutionsregelungen für Sonderzeichen sind dem CPS, Kapitel 3.1.4, zu entnehmen.

3.1.5 Eindeutigkeit von Namen

Vor der Zertifikatausgabe wird die Korrektheit der Angaben zum DN durch die Registrierungsstelle überprüft. Die Eindeutigkeit des resultierenden DN wird von der Registrierungsstelle sichergestellt. Der DN eines Zertifikatinhabers muss eindeutig sein und darf nicht an unterschiedliche Zertifikatinhaber vergeben werden. Falls erforderlich wird eine Laufnummer zum DN hinzugefügt, um die Eindeutigkeit des DN sicherzustellen, z. B. „DN=Peter Muster 2“. Nur wenn ein Zertifikatinhaber mehrere Zertifikate mit unterschiedlicher Schlüsselnutzung besitzt, kann ein DN mehrmals vorkommen.

3.1.6 Erkennung, Authentifizierung und Funktion von Warenzeichen

Die Regelung ist im CPS, Kapitel 3.1.6, beschrieben.

3.2 Identitätsüberprüfung bei Neuantrag

Please find an English translation in the appendix, chapter 10.

3.2.1 Verfahren zur Überprüfung des Besitzes des privaten Schlüssels

Der private Schlüssel wird innerhalb einer sicheren Signaturerstellungseinheit (SSCD) erzeugt. Die entsprechenden Verfahren werden im CPS, Kapitel 3.2.1, beschrieben.

3.2.2 Verfahren bei Zertifikatsanträgen für Organisationen

3.2.2.1 Allgemeine Anforderungen

Die Anforderungen an die Überprüfung der Angaben der Antragsteller und RAs, welche ein Zertifikat im Namen einer Organisation beantragen, richten sich vorliegend nach der Verordnung der Eidgenössischen Steuerverwaltung über Zertifizierungsdienste im Bereich der ElDI-V [8] und insbesondere den Anforderungen der TAV-ElDI-V [9].

Swisscom verlangt von einer Organisation, die einen Antrag auf Ausstellung eines „Saphir" Zertifikats in ihrem Namen stellt, dass sie bzw. ihre Vertreter vor Ausstellung des Zertifikats persönlich in Erscheinung treten und den Nachweis ihrer Identität mit gültigen amtlichen Ausweispapieren erbringt. Im Wesentlichen hat die antragstellende Organisation Dokumente vorzulegen, mit denen Name und Sitz der Organisation festgestellt werden können. Die Einzelheiten ergeben sich aus den folgenden Kapiteln 3.2.2.2- 3.2.2.6.

Zudem prüft Swisscom vor Ausstellung des Zertifikats, ob die Vertreter (oder Organe) der Organisation berechtigt sind, im Namen der Organisation, für die sie tätig sind, ein Zertifikat zu beantragen. Hierfür haben die Vertreter entweder einen gültigen Pass oder eine gültige Schweizer Identitätskarte oder eine für die Einreise in die Schweiz anerkannte, gültige Identitätskare vorzuweisen. In Ausnahmefällen kann ein anderes gültiges amtliches Ausweisdokument mit Unterschriftszug vorgewiesen werden.

Swisscom kann ihre Aufgabe zur Identifikation an Dritte (Registrierungsstellen) delegieren.

Die Organisationen können die Identifikationsprüfung von Mitgliedern ihrer Organisation an eine RA delegieren.

3.2.2.2 Überprüfung der Angaben eines Wirtschaftssubjekts mit Handelsregistereintrag

Benennung der Organisation:

Beschreibung	RDN	Inhalt
Organization	O	Name der Firma gemäss eingereichtem Handelsregisterauszug

Die Berechtigung, im Namen einer im Handelsregister eingetragenen Firma (z.B. AG, GmbH, Einzelfirma mit Jahresumsatz über CHF 100'000) ein Zertifikat zu beantragen, prüft Swisscom mit einem beglaubigten Handelsregisterauszug. Der beglaubigte Handelsregisterauszug darf im Moment der Prüfung nicht älter als drei Monate sein. Die Person, die den Antrag für das Wirtschaftssubjekt stellt, muss darin als Vertretungsberechtigter des Unternehmens genannt sein oder über eine Vollmacht verfügen, die von dem oder den Vertretungsberechtigten des Unternehmens eigenhändig unterzeichnet wurde. Eine Vollmacht ist beispielsweise nötig, wenn die

im Handelsregisterauszug genannte Firma nur gemeinschaftlich vertreten werden kann (z.B. Zeichnungsart „Kollektivunterschrift zu zweien“). Swisscom prüft die Vertretungsberichtigung des Vollmachtgebers anhand des Handelsregisterauszugs.

Zusätzlich prüft Swisscom Zertifikatsanträge für ElDI-V [8] nach folgender Tabelle:

Beschreibung	RDN	Quelle/Inhalt
Organization	O	Beglaubigter Handelsregisterauszug
Organizational Unit	$OU_{0..n}$	Schriftliche Bestätigung durch Vertretungsberechtigten
Organizational Unit	OU_{n+1}	Schriftliche Bestätigung der Funktion des Zertifikats als ElDI-V [8] - Zertifikat zum Zweck von Art. 9 ElDI-V [8]. Falls das Zertifikat nicht auch tatsächlich für diesen Zweck eingesetzt wird („Third Party Services (art. 9 OeIDI)“), ist diese Angabe nicht zulässig (vgl. Ziff. 4.1 TAV-ElDI-V [9])
Common Name	CN	Der CN muss die Angaben vom RDN O enthalten
Locality	L	Beglaubigter Handelsregisterauszug
State/Province	ST	Beglaubigter Handelsregisterauszug
Country	C	Beglaubigter Handelsregisterauszug
EmailAddress	$E_{0..1}$	Schriftliche Bestätigung durch Vertretungsberechtigten

3.2.2.3 Überprüfung der Angaben einer Einzelfirma ohne Handelsregistereintrag

Benennung der Organisation:

Beschreibung	RDN	Inhalt
Organization	O	Name der Einzelfirma nach der eingereichten Eintragungsbescheinigung der ESTV

Der Antragsteller erscheint persönlich gegenüber Swisscom oder bei einer hierfür durch Swisscom berechtigten Registrierungsstelle und legt für die Identitätsprüfung entweder einen gültigen Pass oder eine gültige Schweizer Identitätskarte oder eine für die Einreise in die Schweiz anerkannte, gültige Identitätskarte vor. Zusätzlich muss die Berechtigung, im Namen einer Einzelfirma ein Zertifikat zu beantragen, mit der Eintragungsbescheinigung der ESTV belegt werden.

Zusätzlich prüft Swisscom Zertifikatsanträge für ElDI-V [8] nach folgender Tabelle:

Beschreibung	RDN	Quelle/Inhalt
Organization	O	Eintragungsbescheinigung der ESTV
Organizational Unit	$OU_{0..n}$	Schriftliche Bestätigung durch Vertretungsberechtigten
Organizational Unit	OU_{n+1}	Schriftliche Bestätigung der Funktion des Zertifikats als ElDI-V [8] - Zertifikat zum Zweck von Art. 9 ElDI-V [8]. Falls das Zertifikat nicht auch tatsächlich für diesen Zweck eingesetzt wird („Third Party Services (art. 9 OeIDI)“), ist diese Angabe nicht zulässig
Common Name	CN	Der CN muss die Angaben vom RDN O enthalten
Locality	L	Eintragungsbescheinigung der ESTV
State/Province	ST	Eintragungsbescheinigung der ESTV
Country	C	Eintragungsbescheinigung der ESTV
EmailAddress	$E_{0..1}$	Schriftliche Bestätigung durch Vertretungsberechtigten

3.2.2.4 Überprüfung der Angaben einer einfachen Gesellschaft

Die einfache Gesellschaft nach Art. 530 ff. Obligationenrecht entsteht durch Vertrag. Deren Mitglieder können sowohl natürliche als auch juristische Personen sein. Die einfache Gesellschaft besitzt keine Rechtspersönlichkeit, wird von der Mehrwertsteuer aber als Steuersubjekt betrachtet, weshalb auch in deren Namen ElDI-V [8] - Zertifikate beantragt werden können. Häufigste Erscheinungsform der einfachen Gesellschaft ist die so genannte Arbeitsgemeinschaft (ARGE) im Bauwesen (vertraglicher Zusammenschluss zweier oder mehrerer Baufirmen zur Realisierung eines grösseren Bauprojektes).

Benennung der Organisation:

Beschreibung	RDN	Inhalt
Organization	O	Name der einfachen Gesellschaft nach der eingereichten Eintragungsbescheinigung der ESTV oder nach dem Gesellschaftsvertrag

Die Prüfung erfolgt anhand des Gesellschaftsvertrags und der Eintragungsbescheinigung der ESTV. Der Sitz ergibt sich nicht in jedem Fall aus der Eintragungsbescheinigung der ESTV. Diesfalls sind für die Feststellung des Sitzes andere geeignete Dokumente vorzulegen.

- Die Berechtigung, im Namen einer einfachen Gesellschaft ein Zertifikat zu beantragen, muss mit dem Gesellschaftsvertrag belegt werden. Der Antragsteller muss im Gesellschaftsvertrag als Gesellschafter genannt sein.
- Handelt es sich beim Gesellschafter um eine juristische Person, muss zusätzlich ein beglaubigter Handelsregisterauszug vorgelegt werden. Dieser darf nicht älter als drei Monate sein. Die den Antrag stellende Person muss darin als Vertretungsberechtigte der Gesellschafterin genannt sein oder über eine Vollmacht verfügen, die von dem oder den Vertretungsberechtigten der einfachen Gesellschaft eigenhändig unterzeichnet wurde. Eine Vollmacht ist beispielsweise nötig, wenn die im Handelsregisterauszug genannte Firma nur gemeinschaftlich vertreten werden kann. Die Vertretungsberichtigung der Vollmachtgeberin muss aufgrund des Handelsregisterauszuges geprüft werden.

Zusätzlich prüft Swisscom Zertifikatsanträge für ElDI-V [8] nach folgender Tabelle:

Beschreibung	RDN	Quelle/Inhalt
Organization	O	Eintragungsbescheinigung der ESTV
Organizational Unit	$OU_{0..n}$	Schriftliche Bestätigung durch Vertretungsberechtigten
Organizational Unit	OU_{n+1}	Schriftliche Bestätigung der Funktion des Zertifikats als ElDI-V [8] - Zertifikat zum Zweck von Art. 9 ElDI-V [8]. Falls das Zertifikat nicht auch tatsächlich für diesen Zweck eingesetzt wird („Third Party Services (art. 9 OeIDI)“), ist diese Angabe nicht zulässig
Common Name	CN	Der CN muss die Angaben vom RDN O enthalten
Locality	L	Eintragungsbescheinigung der ESTV
State/Province	ST	Eintragungsbescheinigung der ESTV
Country	C	Eintragungsbescheinigung der ESTV
EmailAddress	$E_{0..1}$	Schriftliche Bestätigung durch Vertretungsberechtigten

3.2.2.5 Überprüfung der Angaben von Gemeinden (Gemeinwesen)

Neben den politischen Gemeinden (Einwohnergemeinden) existieren z.B. auch Bürgergemeinden und Kirchgemeinden. Es lässt sich nicht allgemein festhalten, wer für eine Gemeinde handeln kann. Die Aufsicht über die Gemeinden ist kantonal geregelt und kann deshalb von Kanton zu Kanton unterschiedlich sein. Es gilt die weitere Besonderheit, dass bei der Mehrwertsteuer nicht zwingend die Gemeinde als Ganzes, sondern einzelne Dienststellen, die steuerbare Leistungen erbringen, als Mehrwertsteuerpflichtige eingetragen werden.

Benennung der Organisation:

Beschreibung	RDN	Inhalt
Organization	O	Name der Gemeinde nach dem amtlichen Gemeindeverzeichnis
Organization Unit	OU	Name der Dienststelle, bei ElDI-V [8] nach der eingereichten Eintragungsbescheinigung der ESTV

Die Prüfung erfolgt mittels Kopie der Wahlverfügung (z.B. Gemeindepräsident) oder der Bestätigung durch die zuständige kantonale Behörde. Die Gemeinde muss im amtlichen Gemeindeverzeichnis eingetragen sein.

Zusätzlich prüft Swisscom Zertifikatsanträge für ElDI-V [8] nach folgender Tabelle:

Beschreibung	RDN	Quelle/Inhalt
Organization	O	Eintragungsbescheinigung der ESTV
Organizational Unit	$OU_{0..n}$	Schriftliche Bestätigung durch Vertretungsberechtigten
Organizational Unit	OU_{n+1}	Schriftliche Bestätigung der Funktion des Zertifikats als ElDI-V [8] - Zertifikat zum Zweck von Art. 9 ElDI-V [8]. Falls das Zertifikat nicht auch tatsächlich für diesen Zweck eingesetzt wird („Third Party Services (art. 9 OeIDI)“), ist diese Angabe nicht zulässig
Common Name	CN	Der CN muss die Angaben vom RDN O enthalten
Locality	L	Amtliches Gemeindeverzeichnis
State/Province	ST	Amtliches Gemeindeverzeichnis
Country	C	Schweiz oder Suisse oder Svizzera, oder Landesbezeichnung nach Staatsvertrag (Art. 3 Bst. a Mehrwertsteuergesetz)
EmailAddress	$E_{0..1}$	Schriftliche Bestätigung durch Vertretungsberechtigten

3.2.2.6 Überprüfung der Angaben von anderen, nicht im Handelsregister eingetragenen Wirtschaftssubjekten (z.B. Vereine)

Die Benennung richtet sich nach den Regeln, die für Einzelfirmen gelten:

Beschreibung	RDN	Inhalt
Organization	O	Name nach der eingereichten Eintragungsbescheinigung der ESTV

Die Prüfung erfolgt nach der Eintragungsbescheinigung der ESTV und z. B. den Vereinsstatuten oder anderen Dokumenten. Der Sitz ergibt sich nicht in jedem Fall aus der Eintragungsbescheinigung der ESTV. In diesem Fall sind andere Dokumente notwendig, die geeignet sind, um den Sitz festzustellen.

Die Berechtigung, im Namen eines Wirtschaftssubjektes im Sinn dieser Ziffer ein Zertifikat zu beantragen, muss mit geeigneten Dokumenten nachgewiesen werden. Daraus muss sich ergeben,

welche Organe das Wirtschaftssubjekt gegen aussen vertreten dürfen und welche Person diese Funktion im Zeitpunkt des Antrages innehat.

Zusätzlich prüft Swisscom Zertifikatsanträge für ElDI-V [8] nach folgender Tabelle:

Beschreibung	RDN	Quelle/Inhalt
Organization	O	Eintragungsbescheinigung der ESTV
Organizational Unit	$OU_{0..n}$	Schriftliche Bestätigung durch Vertretungsberechtigten
Organizational Unit	OU_{n+1}	Schriftliche Bestätigung der Funktion des Zertifikats als ElDI-V [8] - Zertifikat zum Zweck von Art. 9 ElDI-V [8]. Falls das Zertifikat nicht auch tatsächlich für diesen Zweck eingesetzt wird („Third Party Services (art. 9 OeIDI)“), ist diese Angabe nicht zulässig
Common Name	CN	Der CN muss die Angaben vom RDN O enthalten
Locality	L	Eintragungsbescheinigung der ESTV oder gemäss oben beschriebenen Dokumenten
State/Province	ST	Eintragungsbescheinigung der ESTV oder gemäss oben beschriebenen Dokumenten
Country	C	Eintragungsbescheinigung der ESTV oder gemäss oben beschriebenen Dokumenten
EmailAddress	$E_{0..1}$	Schriftliche Bestätigung durch Vertretungsberechtigten

3.2.3 Verfahren bei Zertifikatsanträgen von natürlichen Personen

Bei Zertifikatsanträgen von natürlichen Personen identifiziert die RA den Antragsteller, stellt insbesondere sicher, dass ein eindeutiger Distinguished Name (DN) gegeben ist (vgl. auch Kapitel 3.1.2) und prüft alle Attribute, die im Zertifikat aufgenommen werden sollen mit geeigneten Mitteln. Die RA dokumentiert das Verfahren und stellt Swisscom die Unterlagen auf Anfrage zur Verfügung.

Die Identitätsprüfung von natürlichen Personen, welche die Ausstellung eines Organisationszertifikates in eigenem Namen beantragen, richtet sich nach den strengeren Bestimmungen der Kapitel 3.2.2.2 oder 3.2.2.3 (welche den Anforderungen der TAV-ElDI-V [9] genügen).

3.2.4 Nicht überprüfte Informationen

Es werden alle Informationen überprüft, die für die Identitätsprüfung erforderlich sind (Kapitel 3.2). Darüber hinaus werden keine weiteren Informationen überprüft.

3.2.5 Antragsteller mit hohem Risiko

Die Regelungen sind im CPS, Kapitel 3.2.5, beschrieben.

3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung

3.3.1 Routinemässige Zertifikaterneuerung (re-key)

Eine routinemässige Zertifikaterneuerung setzt voraus, dass der Zertifikatinhaber über ein gültiges Zertifikat der zuständigen CA (Zertifikatsklasse „Saphir“) oder einer höherwertigeren CA (Zertifikatsklasse „Diamant“) verfügt.

3.3.2 Zertifikaterneuerung (re-key) nach einer Ungültigerklärung

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

3.4 Identifizierung und Authentifizierung bei einer Ungültigerklärung

Die Details sind dem CPS [8], Kapitel 3.4, zu entnehmen.

4 Betriebsanforderungen für den Zertifikats Lebenszyklus

4.1 Zertifikatantrag

4.1.1 Wer kann ein Zertifikat beantragen

Folgende Personen können ein Zertifikat der Klasse „Saphir“ beantragen:

- natürliche Personen (vgl. Kapitel 3.2.3)
- Organisationen (vgl. Kapitel 3.2.2)

4.1.2 Registrierungsprozess

Ein Zertifikat kann durch Swisscom erst erzeugt werden, wenn der Registrierungsprozess bei einer Registrierungsstelle erfolgreich abgeschlossen wurde. Die Dokumentation des Registrierungsprozesses beinhaltet zumindest:

- signierter Zertifikatantrag
- Identitätsnachweis gemäss Kapitel 3.2;
- Nachweis aller geforderten Attribute gemäss Kapitel 3.1.1;
- Aussage darüber, ob die Informationen im Zertifikat veröffentlicht werden sollen.
  Standardmässig werden die Daten nicht publiziert.
  Bei Zertifikaten, deren Gültigkeitsdauer kürzer ist als das Publikationsintervall der CRL (siehe Kapitel 4.9.7), ist eine Veröffentlichung nicht möglich.

4.2 Bearbeitung von Zertifikatanträgen

4.2.1 Durchführung der Identifikation und Authentifizierung

Die zuständige Registrierungsstelle führt die Identifikation und Authentifizierung eines Antragstellers eines Zertifikats nach den im Kapitel 3.2 beschriebenen Verfahren durch.

4.2.2 Annahme oder Abweisung von Zertifikatanträgen

Zertifikatanträge sind an Registrierungsstelle von Swisscom zu richten. Der Zertifikatsantrag wird von der Registrierungsstelle angenommen, wenn die folgenden Kriterien erfüllt sind:

- Vorlage aller notwendigen Dokumente (siehe Kapitel 4.1.2)
- Zahlung der ggf. festgelegten Gebühr (siehe CPS, Kapitel 9.1).

Nach erfolgreicher Prüfung der obgenannten Kriterien und nach Durchführung der Identifikation und Authentifizierung wird der Zertifizierungsantrag durch Swisscom weiter bearbeitet.

Sollte die Prüfung der obgenannten Kriterien oder die Identifikation und Authentifizierung eines Antragstellers eines Zertifikats nicht erfolgreich sein, wird der Zertifikatsantrag nicht bearbeitet. Der Sachverhalt wird dokumentiert und dem Antragsteller unter Angabe der Gründe mitgeteilt.

4.2.3 Bearbeitungsdauer

Die Bearbeitungsdauer richtet sich nach den Bestimmungen der jeweiligen Registrierungsstelle.

4.3 Zertifikatausstellung

Nach Eingang und erfolgreicher Prüfung (siehe 4.2.2) eines Zertifikatantrags wird:

- sichergestellt, dass ein SSCD gemäss Artikel 3.3.3 gemäss TAV-ZertES [3] eingesetzt wird
- durch Swisscom ein digitales Zertifikat der Klasse „Saphir“ ausgestellt
- das Zertifikat wird dem Antragsteller ausgehändigt, übermittelt oder für ihn hinterlegt.
- der Antragsteller über den korrekten Umgang mit dem kryptografischen Mittel (unter Hinweis auf die zu befolgenden Nutzungsbestimmungen für die Zertifikate) instruiert

4.3.1 Weitere Prüfungen der Zertifizierungsstelle

Die formalen Voraussetzungen für die Ausstellung eines Zertifikats werden durch Swisscom in angemessener Weise überprüft. Weitere Überprüfungen finden nicht statt.

4.3.2 Benachrichtigung des Antragstellers

Der Antragsteller wird von Swisscom nicht über die Zertifikatsausstellung informiert.

4.4 Zertifikat-Akzeptanz

Es gelten die Regelungen in Kapitel 4.4 der CPS.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

Der Anwendungsbereich der im Rahmen dieser CP ausgestellten Zertifikate ist dem Kapitel 1.4 zu entnehmen.

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatinhaber

Durch Annahme des Zertifikats versichert der Zertifikatinhaber allen Teilnehmern im Sinn von Kapitel 1.3 und allen Parteien, die sich auf die Vertrauenswürdigkeit der in dem Zertifikat enthaltenden Informationen verlassen, dass:

- ein angemessenes Verständnis der Anwendung und des Einsatzes von Zertifikaten besteht,
- sämtliche Angaben und Erklärungen des Zertifikatinhabers in Bezug auf die im Zertifikat enthaltenen Informationen der Wahrheit entsprechen,
- zur Erstellung der Signatur ein geeignetes Verfahren angewendet wurde, das dem Signaturprüfer erlaubt, bei der Signaturprüfung Veränderungen festzustellen
- der private Schlüssel geschützt aufbewahrt wird,
- keiner unbefugten Person Zugang zu dem privaten Schlüssel gewährt wird,
- das Zertifikat ausschliesslich in Übereinstimmung mit dieser CP eingesetzt wird,

- das Zertifikat unverzüglich ungültig erklärt wird, wenn die Angaben des Zertifikats nicht mehr stimmen oder der private Schlüssel abhanden kommt, gestohlen oder möglicherweise kompromittiert wurde.

4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Zertifikatprüfer

Jeder, der ein Zertifikat, welches im Rahmen dieser CP ausgestellt wurde, zur Überprüfung einer Signatur oder für die Zwecke der Authentifizierung verwendet, sollte:

- ein grundlegendes Verständnis der Anwendung und des Einsatzes von Zertifikaten besitzen,
- geeignete Komponenten und Verfahren zur Signaturprüfung einsetzen (siehe dazu CPS [8], Kapitel 2.2)
- die entsprechende Sperrliste (CRL) oder OCSP-Antwort überprüfen, bevor er sich auf die Informationen in einem Zertifikat verlässt (die URL, unter der die zugehörige Sperrliste bzw. OCSP veröffentlicht wird, ist im Zertifikat aufgeführt) und
- das Zertifikat ausschliesslich für autorisierte und legale Zwecke in Übereinstimmung mit dieser CP einsetzen.

4.6 Zertifikaterneuerung unter Verwendung des alten Schlüssels (Certificate renewal)

Die Erstellung eines neuen Zertifikates mit dem alten Schlüssel (certificate renewal) wird durch Swisscom für Zertifikate der Klasse „Saphir“ nicht angeboten.

Bei einer Zertifikatserneuerung wird dem Zertifikatinhaber von der zuständigen Registrierungsstelle ein neues Zertifikat basierend auf einem neuen Schlüsselpaar ausgestellt (Re-Key-Verfahren, siehe Kapitel 4.7).

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

Bei einer Zertifikaterneuerung wird grundsätzlich ein neues Schlüsselpaar erstellt.

Ein neues Zertifikat wird immer auf einer neuen sicheren Signaturerstellungseinheit ausgestellt. Bei der Verwendung eines HSM wird im HSM ein neues Schlüsselpaar erzeugt. Es werden die Schlüssellänge und der Algorithmus verwendet, der zu dem jeweiligen Zeitpunkt aktuell ist und gemäss geltender CPS [6] einzusetzen sind. Der Zertifikatinhaber oder die zuständige RA hat zu bestätigen, dass die im Zertifikat enthaltenen Informationen unverändert bleiben und die anlässlich der Zertifikatsausstellung vorgelegten Dokumente noch gültig sind. Das alte Zertifikat wird nach Ausstellung des neuen Zertifikats nicht ungültig erklärt und bleibt bis zum Ablauf der Gültigkeitsdauer gültig.

4.7.1 Gründe für Re-Key

Eine Zertifikaterneuerung mit einem neuen Schlüsselpaar (re-key) kann dann ausgeführt werden, wenn:

- die Gültigkeit des Zertifikats abläuft
- die gesetzlichen Grundlagen gemäss ElDI-V [12] eine Anpassung erfordern
- die verwendete Schlüssellänge oder ein eingesetzter Algorithmus als nicht mehr ausreichend betrachtet wird.

4.7.2 Beantragung Re-Key

Eine Zertifikaterneuerung mit einem neuen Schlüsselpaar (re-key) wird grundsätzlich durch den Zertifikatinhaber beantragt.

4.7.3 Ablauf Re-Key

Der Ablauf der Zertifikaterneuerung mit einem neuen Schlüsselpaar (re-key) entspricht den Regelungen unter Kapitel 4.3, für die Identifizierung und Authentifizierung bei der Re-Zertifizierung gelten die Regelungen gemäss Kapitel 3.3.1.

4.8 Zertifikatmodifizierung

Die Modifizierung von Zertifikaten der Klasse „Saphir“ wird nicht angeboten.

Müssen Attribute des Zertifikates angepasst werden, wird ein neues Zertifikat basierend auf einem neuen Schlüsselpaar, ausgestellt (Re-Key-Verfahren, siehe Kapitel 4.7). Anpassungen, die sich alleine aufgrund geänderter gesetzlicher Grundlagen ergeben, können ohne Antrag und Neuidentifikation des Zertifikatsinhabers durchgeführt werden, sofern keine Namenselemente (DN, SAN) angepasst werden und das Ablaufdatum des Zertifikats nicht später als fünf Jahre nach der Identifikation ist.

4.9 Ungültigerklärung und Suspendierung von Zertifikaten

In diesem Abschnitt werden die Umstände erläutert, unter denen ein Zertifikat ungültig erklärt werden muss. Eine Suspendierung (zeitliche Aussetzung) von Zertifikaten wird nicht vorgenommen. Einmal ungültig erklärte Zertifikate können nicht erneuert oder verlängert werden.

Für Zertifikate mit einer Gültigkeitsdauer kürzer als das Publikationsintervall der CRL (siehe Kapitel 4.9.7), wird keine Ungültigerklärung angeboten. Die zugehörigen Schlüsselpaare dürfen nur für eine Signatur verwendet und müssen danach gelöscht werden.

4.9.1 Gründe für eine Ungültigerklärung

Zertifikate müssen von Swisscom oder der zuständigen RA ungültig erklärt werden, wenn:

- der Zertifikatsinhaber oder die juristische Person oder Organisation, die dieser vertritt einen entsprechenden Antrag stellt, oder
- Swisscom oder der RA mindestens einer der folgenden Gründe bekannt wird:
  - Ein Zertifikat enthält Angaben, die nicht (mehr) gültig sind.
  - Das Zertifikat ist unrechtmässig erlangt worden.
  - Das Zertifikat keine Gewähr mehr bietet für die Zuordnung eines Signaturprüfschlüssels zu einer bestimmten Person.
  - Der private Schlüssel des Zertifikatinhabers wurde geändert, verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
  - Der Zertifikatinhaber hat seine Berechtigungsgrundlage (siehe 1.3.3) verloren.
  - Der Zertifikatinhaber hält diese CP nicht ein.
  - Die zuständige Registrierungsstelle (RA) hält diese CP oder das CPS [6] nicht ein.
  - Der Zertifikatinhaber benötigt das betroffene Zertifikat nicht mehr.
  - Der Zertifizierungsbetrieb wird eingestellt.

- Der Zertifikatinhaber kommt seiner Zahlungspflicht für die Gebühren auch nach mehrmaliger Aufforderung nicht nach.
- Die Übergangsbestimmungen von ElDI-V [12] Artikel 14 dies erfordern.

4.9.2 Wer kann die Ungültigerklärung vornehmen

Zertifikate können grundsätzlich nur von der ausstellenden RA oder von Swisscom ungültig erklärt werden. Jeder Zertifikatinhaber kann von der zuständigen RA, die sein Zertifikat erstellt hat, unter Angabe von Gründen verlangen, dass diese ein für ihn ausgestelltes Zertifikat ungültig erklärt. Verfahren für eine Ungültigerklärung eines Zertifikats sind dem zugehörigen CPS, Kapitel 4.9, zu entnehmen. Voraussetzung für die Akzeptanz einer Ungültigerklärung des Zertifikats ist eine erfolgreiche Identifizierung und Authentifizierung des Zertifikatinhabers entsprechend Kapitel 3.4.

4.9.3 Ablauf einer Ungültigerklärung eines Zertifikats

Sind die Voraussetzungen für eine Ungültigerklärung eines Zertifikats erfüllt, wird das Zertifikat unverzüglich widerrufen.

Das Zertifikat kann auf folgende Arten widerrufen werden:

- Persönliche Vorsprache bei der Registrierungsstelle mit Angabe der Autorisierungs-information bzw. Identitätsprüfung nach Kapitel 3.4.
- Telefon-Anruf bei der zuständigen RA mit Angabe der Autorisierungsinformation.
- Übersendung eines unterzeichneten Widerrufsantrags unter Angabe der Seriennummer des Zertifikates per Post. Zur Verifikation der Identität wird der Zertifikatsinhaber zurückgerufen.
- Ausserhalb der Geschäftszeiten der zuständigen RA kann die Swisscom Hotline unter 0800 724 724 kontaktiert werden, die dann die Ungültigerklärung initialisiert. Zur Verifikation der Identität wird der Zertifikatsinhaber zurückgerufen.

4.9.4 Fristen für den Zertifikatinhaber

Der Zertifikatinhaber muss unverzüglich die zuständige RA oder Swisscom benachrichtigen und die Ungültigerklärung des eigenen Zertifikats veranlassen, wenn Gründe (siehe Kapitel 4.9.1) für eine Ungültigerklärung vorliegen.

4.9.5 Fristen für die Zertifizierungsstelle

Swisscom bearbeitet einen Auftrag für eine Ungültigerklärung eines Zertifikats unverzüglich.

4.9.6 Anforderungen zur Kontrolle der CRL durch den Zertifikatprüfer

Es gelten die Regelungen gemäss Kapitel 4.5.2.

4.9.7 Aktualisierung der CRL's

Die CRL wird alle 2 Stunden nachgeführt.

4.9.8 Maximale Latenzzeit für CRL's

Nach einer Veränderung wird eine neue CRL innerhalb von 2 Stunden veröffentlicht.

4.9.9 Verfügbarkeit von Online-Ungültigkeits/Status-Überprüfungsverfahren

Swisscom bietet mehrere Online-Verfahren an, mit denen die Gültigkeit eines Zertifikats überprüft werden kann. Es müssen dabei alle Zertifikate erfasst werden, die von der Zertifizierungsstelle ausgestellt worden sind. Details sind dem Kapitel 4.10 der CPS zu entnehmen.

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

4.9.10 Anforderungen an Online-Ungültigkeits/Status-Überprüfungsverfahren

Die Standards sind den Abschnitten 3 (CRL-Profil) und 4 (OCSP-Profil) des Addendums zum CPS [7] zu entnehmen.

4.9.11 Andere verfügbare Formen der Ungültigkeitsbekanntmachung

Swisscom bietet keine anderen Verfahren zur Ungültigkeitsbekanntmachung an als in Kapitel 4.10 der CPS aufgeführt.

4.9.12 Kompromittierung von privaten Schlüsseln

Bei einer Kompromittierung des privaten Schlüssels ist das entsprechende Zertifikat unverzüglich für ungültig erklären zu lassen.

Bei einer Kompromittierung des privaten Schlüssels einer CA werden alle von ihr ausgestellten Zertifikate widerrufen.

4.9.13 Gründe für eine Suspendierung

Eine Suspendierung von Zertifikaten der Klasse „Saphir“ wird nicht angeboten.

4.10 Dienst zur Statusabfrage von Zertifikaten

Die Details zum Verfahren, Verfügbarkeit und dessen Merkmale sind dem CPS, Kapitel 4.10, zu entnehmen.

4.11 Beendigung des Vertragsverhältnisses durch den Zertifikatinhaber

Die Dauer des Vertragsverhältnisses ergibt sich aus der im Zertifikat angegebenen Gültigkeitsdauer (i.d.R. 3 Jahre).

4.12 Schlüsselhinterlegung und -wiederherstellung

Schlüsselhinterlegung und -wiederherstellung (Key-Escrow and Recovery) werden für Signaturschlüssel der Klasse „Saphir“ nicht angeboten.

Beim Einsatz von HSM darf der Signaturschlüssel für ein Backup in geeigneter Weise exportiert werden, sofern der Signaturschlüssel gleichwertig geschützt ist wie im SSCD, und ausgeschlossen werden kann, dass der Signaturschlüssel ausserhalb des SSCD genutzt werden kann.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen

Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen sind dem CPS, Kapitel 5, zu entnehmen.

6 Technische Sicherheitsmassnahmen

Technische Sicherheitsmassnahmen sind dem CPS, Kapitel 6, zu entnehmen.

7 Profile für Zertifikate, Widerrufslisten und Online-Statusabfragen

Zertifikatsprofile, Widerrufslisten (CRL) und Online-Statusabfragen (OCSP) sind im Addendum zum CPS [9] detailliert beschrieben.

7.1 Zertifikatprofil

Ein von Swisscom ausgegebenes Zertifikat der Klasse „Saphir" umfasst folgende, im X.509 v3 Standard definierten und gemäss ElDI-V [8] sowie TAV-ZertES verlangten Pflichtfelder:

- X.509 Version des Zertifikates
- Zertifikatseriennummer (Seriennummer)
- Objectidentifier des Hash- und Signaturalgorithmus
- Name der CA (Issuer Distinguished Name)
- Gültigkeitsdauer (von – bis)
- Name des Zertifikatinhabers (Subject Distinguished Name)
- Public Key des Zertifikatinhabers

Die Details des Zertifikatsprofiles sind dem Addendum zum CPS [7] Kapitel 2 zu entnehmen.

7.1.1 Zertifikaterweiterungen

Es sind folgende, im X.509 v3 Standard definierten und gemäss TAV-ZertES verlangten Erweiterungen vorhanden:

- authorityKeyIdentifier (nicht kritisch)
- subjectKeyIdentifier (nicht kritisch)
- Verwendungszweck des Zertifikats (kritisch)
- Zertifizierungsrichtlinie (nicht kritisch)
- CRL Distribution Point (nicht kritisch)
- Zugangspunkt zum Zertifikat der CA (nicht kritisch)

Zusätzlich sind folgende im X509 v3 Standard definierten Erweiterungen möglich:

- Issuer alternative Name (nicht kritisch), <RFC konforme Attribute>
- Subject alternative Name (nicht kritisch), <RFC konforme Attribute>

8 Konformitätsprüfung (Compliance Audit) und andere Assessments

Swisscom und die RA-Vertragspartner, welche digitale Zertifikate zur Erstellung fortgeschrittener elektronischer Signaturen ausstellen, sind verpflichtet, alle ihre Abläufe dieser CP und dem CPS [6] entsprechend auszugestalten. Swisscom erfüllt alle Vorgaben des ZertES und den daraus abgeleiteten technischen und administrativen Vorschriften. Die Einhaltung wird gemäss TAV-ZertES, Kapitel 2 „System für die Anerkennung der CSP" durch die von einer durch die schweizerische

Akkreditierungsstelle akkreditierte Anerkennungsstelle überprüft. Siehe dazu auch https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas/pki.html.

Die Einhaltung der Vorgaben der Eidgenössischen Steuerverwaltung für digitale Zertifikate zur Erstellung fortgeschrittener elektronischer Signaturen gemäss ElDI-V [8] wird durch eine unabhängige interne Revision jährlich überprüft und festgehalten.

8.1 Intervall und Umstände der Überprüfung

Da die „Saphir-CA“ in die Prozesse und physikalische Infrastruktur der nach ZertES zertifizierten Umgebung der Swisscom eingebettet ist, profitiert diese von den jährlich wiederkehrenden Audits der Anerkennungsstelle. Zusätzlich ist Swisscom gemäss TAV-ZertES Kapitel 3.2 „Organisation und operative Grundsätze“, Absätze c und d, verpflichtet, jährlich eine Überprüfung durch eine interne Kontrollstelle (internes Audit) durchzuführen.

Integrierter Bestandteil dieser Prüfung sind auch die RA Vertragspartner (Delegation der RA-Tätigkeit gemäss Art. 8 Abs. 4 ZertES [1]).

8.2 Identität und Qualifikation der Überprüferin

Die jährlich wiederkehrende Konformitätsprüfung wird durch eine von Swisscom unabhängige Unternehmung durchgeführt.

Die Funktion der internen Revision wird durch eine qualifizierte externe Unternehmung auf Mandatsbasis durchgeführt.

8.3 Verhältnis von Überprüferin zu Überprüfter

Die interne Revision sowie die Anerkennungsstelle sind unabhängige Firmen, die auf Mandatsbasis die Prüfungen gemäss den gesetzlichen und regulatorischen Vorgaben vornehmen. Die externen und die internen Auditoren sprechen sich in der Planung ab. Die Koordination erfolgt durch den ISO der Swisscom Digital Certificate Services. Das Reporting richtet sich an die Serviceleitung und Legal & Compliance.

8.4 Überprüfte Bereiche

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

Die internen Auditoren erstellen in Absprache mit den externen Auditoren einen Prüfplan für die Prüfhandlungen.

8.5 Mängelbeseitigung

Aufgedeckte Mängel werden in Abstimmung mit den Auditoren und der überprüften Zertifizierungs- bzw. Registrierungsstelle zeitnah behoben: Schwerwiegende Mängel mit hohem Risiko innert 2 Wochen, alle anderen innerhalb 6 Monaten.

8.6 Veröffentlichung der Ergebnisse

Anleitungen zur Behebung oder allfällige Umgehungsmassnahmen zu gravierenden Mängeln werden den Betroffenen umgehend bekannt gemacht.

Eine allgemeine Veröffentlichung der Prüfungsergebnisse ist nicht vorgesehen.

9 Rahmenvorschriften

Die Regelungen sind dem CPS, Kapitel 9, zu entnehmen.

10 Appendix: English Translation of the Identification Procedures

„3.2 Initial Identity Verification“

„3.2.1 Method for proving Possession of the Private Key“

The private key is generated in a secure signature creation device (SSCD). The relevant procedures are described in chapter 3.2.1 of the CPS [6].

„3.2.2 Procedure for Certificate Applications for Organizations”

„3.2.2.1 General Requirements”

The requirements for the verification of information provided by the applicant and RAs, which apply for a certificate on behalf of an organization, are governed by the regulation of the Federal Tax Administration (FTA) on certification services in the field of the Ordinance of the FDF on Electronic Data and Information (OeIDI [8]) and in particular the requirements of the technical and administrative regulations on certification services in the field of OeIDI in connection with the issuance of certificates based on advanced signatures (TAR OeIDI [9]).

Swisscom demands from an organization that requests the issuance of a "Sapphire" certificate on their behalf that they or their representatives appear in person before issuing the certificate and provide proof of their identity with valid official identity documents. Essentially, the applicant organization must submit documents that assert name and place of business of the organization. The details are contained in the following chapters 3.2.2.2 - 3.2.2.6.

Before issuing the certificate Swisscom also checks that the representative (or bodies) of the organization are entitled to apply for a certificate on behalf of the organization for which they work. For this purpose the representatives have to show either a valid passport or a valid Swiss identity card or a valid ID card authorizing entry into Switzerland. In exceptional cases, any other valid official identification document with handwritten signature may be presented.

Swisscom may delegate the task of identification to third parties (registries).

Organizations may delegate the identification check of members of their organization to an RA.

„3.2.2.2 Verification of the Information of a Business Entity with Entry in the Commercial Register”

Classification of the organization:

Description	RDN	Content
Organization	O	Name of the company in accordance with submitted extract from the Commercial Register

The permission to apply for a certificate on behalf of the registered company (e.g. AG, GmbH, sole proprietorship with annual turnover in excess of CHF 100,000), is checked by Swisscom using a certified extract from the commercial register. The certified extract from the commercial register must not be older than three months at the time of testing. The person who submits the application for the business entity must be called therein as authorized representative of the company or have a power of attorney, signed by hand by the owner or authorized representative of the company. A power of attorney, for example, is necessary if the company which is mentioned in the extract from the Commercial Register, can only act jointly (e.g. mode of signature "joint signature in pairs"). Swisscom checks representation rectification of the principal on the basis of the extract from the commercial register.

In addition, Swisscom checks certificate requests for OeIDI according to the following table:

Description	RDN	Source/Content
Organization	O	Certified extract from the commercial register
Organizational Unit	$OU_{0..n}$	Written confirmation by the authorized representative
Organizational Unit	OU_{n+1}	Written confirmation of the function of the certificate as OeIDI certificate for the purpose of art. 9 OeIDI. If the certificate is not actually used for this purpose ("Third Party Services (art. 9 OeIDI)"), this information is not allowed (see. para. 4.1 TAR OeIDI)
Common Name	CN	The CN must contain the information from the RDN O
Locality	L	Certified extract from the commercial register
State/Province	ST	Certified extract from the commercial register
Country	C	Certified extract from the commercial register
EmailAddress	$E_{0..1}$	Written confirmation by the authorized representative

„3.2.2.2 Verification of the Information of a sole Proprietorship with no Entry in the Commercial Register"

Naming of the organization:

Description	RDN	Content
Organization	O	Name of the sole proprietorship according to the submitted certificate of registration of the FTA

The applicant appears in person with Swisscom or with a registrar authorized by Swisscom and submits either a valid passport or a valid Swiss identity card or a valid ID card authorizing entry into Switzerland. Additional, the permission to apply for a certificate on behalf of a sole proprietorship must be assigned by the registration certificate of the FTA.

In addition, Swisscom checks certificate requests for OeIDI according to the following table:

Description	RDN	Source/Content
Organization	O	Registration certificate of the FTA
Organizational Unit	$OU_{0..n}$	Written confirmation by the authorized representative
Organizational Unit	OU_{n+1}	Written confirmation of the function of the certificate as OeIDI certificate for the purpose of art. 9 OeIDI. If the certificate is not actually used for this purpose ("Third Party Services (art. 9 OeIDI)"), this information is not allowed (see. para. 4.1 TAR OeIDI)
Common Name	CN	The CN must contain the information from the RDN O
Locality	L	Registration certificate of the FTA
State/Province	ST	Registration certificate of the FTA
Country	C	Registration certificate of the FTA
EmailAddress	$E_{0..1}$	Written confirmation by the authorized representative

„3.2.2.2 Verification of the Information of a Simple Partnership"

The simple partnership in accordance with Article 530 et seq. Code of Obligations is created by contract. Their members can be both natural and legal persons. The simple partnership has no legal personality, but is considered as a tax subject by the VAT, why OeIDI certificates can also be requested on their behalf. Most common appearance of simple partnership is the so-called joint venture (JV) in the construction industry (contractual merger of two or more construction companies for the realization of a larger construction project).

Naming of the organization:

Description	RDN	Content
Organization	O	Name of the simple partnership according to the submitted certificate of registration of the FTA or according to the partnership contract

The verification is performed based on the partnership contract and the registration certificate of the FTA. The place of business does not in any case result from the registration certificate of the FTA. In this case any other appropriate document for the determination of the place of business must be submitted.

- The entitlement to apply for a certificate on behalf of a single partnership must be subject to the partnership contract. The applicant must be mentioned in the partnership contract as a partner.
- If the partner is a legal entity, a certified extract from the commercial register must be submitted in addition. This must not be older than three months. The applicant must therein be mentioned as authorized representative of the partner or have a power of attorney, signed by hand by the owner or authorized representative of simple partnership. A power of attorney, for example, is necessary if the company which is mentioned in the extract from the Commercial Register, can only act jointly. Swisscom checks representation rectification of the principal based on the extract from the commercial register.

In addition, Swisscom checks certificate requests for OeIDI according to the following table:

Description	RDN	Source/Content
Organization	O	Registration certificate of the FTA
Organizational Unit	$OU_{0..n}$	Written confirmation by the authorized representative
Organizational Unit	OU_{n+1}	Written confirmation of the function of the certificate as OeIDI certificate for the purpose of art. 9 OeIDI. If the certificate is not actually used for this purpose ("Third Party Services (art. 9 OeIDI)"), this information is not allowed (see. para. 4.1 TAR OeIDI)
Common Name	CN	The CN must contain the information from the RDN O
Locality	L	Registration certificate of the FTA
State/Province	ST	Registration certificate of the FTA
Country	C	Registration certificate of the FTA
EmailAddress	$E_{0..1}$	Written confirmation by the authorized representative

„3.2.2.2 Verification of the Information of Communities"

In addition to the political communities (municipalities) also "Bürgergemeinden" and civil parishes exist. It cannot be generally determined, who can act on behalf of a community. The supervision of communities is regulated on a cantonal basis and may therefore differ from canton to canton. It is the further characteristic that with VAT not necessarily the community as a whole, but individual departments providing the taxable services, are registered as VAT payers.

Naming of the organization:

Description	RDN	Content
Organization	O	Name of the community according to the official community directory
Organization Unit	OU	Name of the department, for OeIDI according to the submitted certificate of registration of the FTA

The verification is based on a copy of the certification of the election (e.g. mayor) or the confirmation by the responsible cantonal authorities. The community must be registered on the official community directory.

In addition, Swisscom checks certificate requests for OeIDI according to the following table:

Description	RDN	Source/Content
Organization	O	Registration certificate of the FTA
Organizational Unit	$OU_{0..n}$	Written confirmation by the authorized representative
Organizational Unit	OU_{n+1}	Written confirmation of the function of the certificate as OeIDI certificate for the purpose of art. 9 OeIDI. If the certificate is not actually used for this purpose ("Third Party Services (art. 9 OeIDI)"), this information is not allowed (see. para. 4.1 TAR OeIDI)
Common Name	CN	The CN must contain the information from the RDN O
Locality	L	Official community directory
State/Province	ST	Official community directory
Country	C	Schweiz or Suisse or Svizzera, or country name according to international treaty (Art. 3 let. a VAT law)
EmailAddress	$E_{0..1}$	Written confirmation by the authorized representative

„3.2.2.2 Verification of the Information of other, not the registered Business Entities (eg Associations)

The Naming is subject to the rules that apply to individual companies:

Description	RDN	Content
Organization	O	Name according to the submitted certificate of registration of the FTA

The verification is performed according to the registration certificate of the FTA or the articles of the association or other documents. The place of business does not in any case result from the registration certificate of the FTA. In this case any other appropriate document for the determination of the place of business must be submitted.

The authorization to apply for a certificate on behalf of a business entity in the sense of this paragraph must be proven by appropriate documents. These documents must show what bodies may represent the business entity to outside and which person is holding this function at the time of the application.

In addition, Swisscom checks certificate requests for OeIDI according to the following table:

Description	RDN	Source/Content
Organization	O	Registration certificate of the FTA
Organizational Unit	$OU_{0..n}$	Written confirmation by the authorized representative
Organizational Unit	OU_{n+1}	Written confirmation of the function of the certificate as OeIDI certificate for the purpose of art. 9 OeIDI. If the certificate is not actually used for this purpose ("Third Party Services (art. 9 OeIDI)"), this information is not allowed (see. para. 4.1 TAR OeIDI)
Common Name	CN	The CN must contain the information from the RDN O
Locality	L	Registration certificate of the FTA or under the above-described documents
State/Province	ST	Registration certificate of the FTA or under the above-described documents
Country	C	Registration certificate of the FTA or under the above-described documents
EmailAddress	$E_{0..1}$	Written confirmation by the authorized representative

„3.2.3 Procedures for Certificate Applications from natural persons"

With certificate applications from natural persons, the RA identifies the applicant, ensures in particular that a unique Distinguished Name (DN) is given (see chapter 3.1) and checks all the attributes to be included in the certificate by appropriate means. The RA documents the process and upon request provides Swisscom with the documents.

The identity verification of the natural persons who apply for issuance of an organization certificate in their own name, is subject to the stringent provisions of chapters 3.2.2.2 or 3.2.2.3 (which comply with the requirements of TAR OeIDI).

„3.2.4 Non-verified Information"

All information required for the identity check is examined (section 3.2.2). No additional information is examined.