Swisscom Digital Certificate Services

Certificate Policy (CP)

Zertifikatsklasse „Diamant“ (qualifiziert)

Übersicht	Certificate Policy für qualifizierte Zertifikate der Klasse „Diamant“ der Swisscom Digital Certificate Services.
Name	CP_Diamant_2_16_756_1_83
Version	2.7
Freigabe	10.10.2017
Ablauf	28.02.2018 (Ersatz durch CP/CPS_Diamant_Saphir_v3.0)
Klassifizierung	Public
OID der CP	2.16.756.1.83.11.0 (Diamant CA 2)
Zugehörige CPS	CPS Swisscom Digital Certificate Services (OID 2.16.756.1.83.2.1)
Name der CA	Swisscom Diamant CA 2 (OID 2.16.756.1.83.11)
Inhaber der CA	Swisscom (Schweiz) AG
Sprache	Deutsch (rechtlich verbindliche Originalversion)
Beginn der CP Konformitätsprüfung	1. Januar 2011 (Swisscom Diamant CA 2)
Dokumenten Freigabe	Governance Board der Swisscom Digital Certificate Services

Änderungskontrolle

Version	Datum	Ausführende Stelle	Bemerkungen/Art der Änderung
2.0	04. Nov. 2011	Projektteam	Ergänzungen SHA-256, Unterscheidung beinhaltend CA 1 (ersetzend) und CA 2 (neu)
2.1	02. Sep. 2014	Kerstin Wagner	Review und Überarbeitung
2.2	27.10.2014	Patrick Graber	Ergänzung All-in Signing Service
2.3	29.12.2014	Stéphane Vaucher (LR ENT)	Generelle Anpassungen aus Legal Sicht (hauptsächlich i.Z.m. einerseits All-in Signing Service und andererseits allgemeiner Verständlichkeit des Dokuments als Vertragsbestandteil)
2.4	06.10.2015	Kerstin Wagner	Review 2015
2.5	24.05.2016	Kerstin Wagner	Ergänzung der engl. Übersetzung des Identifikations-prozesses; Auslagerung der Beschreibungen der CA der 1. Generation (CA 1) in ein eigenständiges Dokument; Review und Update 2016
2.6	06.01.2017	H-P Waldegger	Anpassungen an neue Identifikationsvorschriften gem. ZertES Ausgabe vom 18. März 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 und anderer Anwendungen digitaler Zertifikate (auch genannt: 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 und anderer Anwendungen digitaler Zertifikate (auch genannt: Verordnung über die elektronische Signatur) vom 3. Dezember 2004 (Stand am 1. August 2011)

[3] SR 943.032.1, TAV: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate 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

[8] CPS Swisscom Digital Certificate Services, OID 2.16.756.1.83.2.1

[9] Addendum zum CPS [8]: Profile der Zertifikate, Sperrlisten (CRL) und Online Statusabfragen

[10] Nutzungsbestimmungen „Diamant“

[11] CEN/TS 419 241: Security Requirements for Trustworthy Systems supporting Server Signing

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

[13] SR 955.0, Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismus-finanzierung (Geldwäschereigesetz, GwG)

[14] 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 (Zertifizierungsrichtlinien, nachfolgend CP) von Swisscom Digital Certificate Services zur Ausgabe von qualifizierten Zertifikaten im Sinne des schweizerischen Bundesgesetzes über die elektronische Signatur (ZertES [1]) und den daraus abgeleiteten technischen und administrativen Ausführungsbestimmungen in der VZertES [2] und der TAV [3].

Die CP erlaubt Benutzern und Dritten, welche dem Zertifikat vertrauen (Relying Parties), die Vertrauenswürdigkeit der durch Swisscom (Schweiz) AG (nachfolgend Swisscom) und ihren Vertragspartnern ausgestellte Zertifikate abzuschätzen.

Ein Zertifikat ist eine elektronische Bescheinigung, mit der ein öffentlicher kryptografischer Schlüssel einer Person 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 „qualifiziert" in Bezug auf elektronische Signaturen und Zertifikate bedeutet, dass ein Dienstanbieter die Vorgaben des Bundesgesetzes über die elektronische Signatur (ZertES [1]), der dazugehörigen Verordnung (VZertES [2]) und der technischen und administrativen Vorschriften über Zertifizierungsdienste im Bereich der qualifizierten elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (TAV [3]) erfüllt. Die Einhaltung dieser Vorgaben wird durch eine von der Schweizerischen Akkreditierungsstelle (SAS) akkreditierte Anerkennungsstelle geprüft. Danach ist die anerkannte Anbieterin von Zertifizierungsdiensten (CSP) berechtigt, Secure Signature Creation Devices (SSCD) und Zertifikate für die Erstellung und Überprüfung von qualifizierten elektronischen Signaturen im Sinne von Art. 2 Bst. e ZertES [1] anzubieten.

Mit dem am 1.1.2005 in Kraft getretenen schweizerischen Bundesgesetz über die elektronische Signatur wurde auch Art. 14 Abs. 2bisObligationenrecht (OR; SR 220) eingeführt, der die qualifizierte elektronische Signatur der eigenhändigen Unterschrift gleichstellt, womit es möglich wird, Willenserklärungen (insbesondere für den Abschluss von Verträgen) auch in Bereichen, in welchen die Schriftform im Sinn von Art. 12 ff. OR vorgeschrieben ist, mit qualifizierter elektronischer Signatur abzugeben, soweit nicht abweichende gesetzliche oder vertragliche Form- oder Zustellungsvorschriften bestehen. Daneben kann die qualifizierte Signatur auch für den Herkunftsnachweis (Authentizität) und zum Schutz vor Veränderungen (Integrität) eingesetzt werden. Art. 14 Abs. 2bis OR lautet wie folgt:

> „Der eigenhändigen Unterschrift gleichgestellt ist die qualifizierte elektronische Signatur, die auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 19. Dezember 2003 über die elektronische Signatur beruht. Abweichende gesetzliche oder vertragliche Regelungen bleiben vorbehalten."

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. Für die höchste Zertifikatklasse, das qualifizierte Zertifikat, muss eine Person bei einer Registrierungsstelle persönlich in Erscheinung treten und alle im Zertifikat vermerkten Daten mit einem amtlichen Ausweis und eventuellen zusätzlichen Bescheinigungen belegen. 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 „Diamant“. Diese Klasse erfüllt die Anforderungen, welche das ZertES [1] an die qualifizierten Zertifikate stellt.

Für alle Zertifikate, die dieser CP entsprechen, ist der Objekt Bezeichner (OID) gemäss X.509 dieser CP im Zertifikat vermerkt. Somit wird diese CP an das Zertifikat der Klasse „Diamant“ gebunden.

1.1 Überblick

Diese CP wurde von Swisscom zu folgendem Zweck erstellt:

- Erfüllung der Anforderungen an einen Certificate Service Provider (CSP) von qualifizierten Zertifikaten gemäss ZertES [1].
- Beschreibung der Dienstleistungen, Rollen, Einschränkungen und Verpflichtungen bei der Verwendung von qualifizierten Zertifikaten der Swisscom.
- Sicherstellung der Interoperabilität bei der Benutzung qualifizierter Zertifikate der Swisscom.

Die Struktur dieser 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 [12]

Um die internationale Zusammenarbeit mit anderen Zertifizierungsstellen zu ermöglichen, wird ferner eine englische Übersetzung der CPS veröffentlicht sowie gewisse Teile dieser CP ins Englische übersetzt (siehe Appendix, Kap. 10); massgeblich ist in jedem Fall die deutsche Version in der jeweils aktuellen Fassung.

1.2 Identifikation des Dokuments

Identifikation:

- Titel: Swisscom Digital Certificate Services – Zertifizierungsrichtlinie (CP) für die Zertifikatsklasse „Diamant“
- Version: 2.7
- Object Identifier (OID) für diese CP: 2.16.756.1.83.11.0

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 Website des BAKOM eingesehen 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 qualifizierte Zertifikate („Diamant“). 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 CAs der Swisscom Digital Certificate Services aus.

Für den Betrieb der CA und die Funktionentrennung gelten die Vorgaben der TAV [3].

1.3.2 Registrierungsstellen – Registration Authorities (RA)

Die Registrierungsstellen sind im Kapitel 1.3.2 der zugehörigen CPS [8] beschrieben

1.3.3 Zertifikatinhaber (Subscriber)

Ein qualifiziertes Zertifikat kann nur auf eine natürliche Person ausgestellt werden. Die natürliche Person kann allerdings berechtigt sein, eine juristische Person oder Organisation zu vertreten. In diesem Fall ist es möglich, die Eigenschaften dieser Person und den Namen der juristischen Person im Zertifikat zu nennen.

Die natürliche Person wird unter Vorlage ihres amtlichen Ausweises als Zertifikatinhaber gegenüber der RA registriert und sie hat sich zu verpflichten, die Nutzungsbestimmungen [10] einzuhalten.

1.3.4 Zertifikatprüfer (Relying Parties)

Die Zertifikatprüfer sind im Kapitel 1.3.4 der zugehörigen CPS [8] beschrieben

1.3.5 Weitere Teilnehmer

Die weiteren Teilnehmer sind im Kapitel 1.3.5 der zugehörigen CPS [8] 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 als Willensäusserung, als Herkunftsnachweis und zum Schutz von Veränderungen verwendet werden.

Zusätzlich können die Zertifikatsangaben für die Abfrage von Statusinformationen der ungültig erklärten Zertifikate bei Swisscom verwendet werden.

1.4.2 Untersagte Zertifikatnutzung

Grundsätzlich ist mit einem qualifizierten Zertifikat lediglich das Signieren erlaubt. Alle anderen Nutzungen sind 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 [8], Kapitel 9.11.

1.6 Schlüsselwörter und Begriffe

Schlüsselwörter und Begriffe sind Abschnitt 1.6 der CPS [8] zu entnehmen.

1.7 Abkürzungen

AIS	All-in Signing Service
BCP	Business Continuity Plan
CA	Certification Authority
CN	Common Name, als Teil des DN
CP	Certificate Policy, Zertifizierungsrichtlinien
CPS	Certificate Practice Statement, Aussage über die Zertifizierungsrichtlinien
CSP	Certificate Service Provider, Anbieter von Zertifizierungsdiensten
CRL	Certificate Revocation List
DN	Distinguished Name gemäss RFC 3739
E-RA	Enterprise-Registration Authority, Registrierungsstelle bei einem RA Partner
HSM	Hardware Security Module
ISO	Information Security Officer, IT Sicherheitsverantwortlicher
IVA	Identity Validation Authority, Identitätsprüfstelle
LDAP	Lightweight Directory Access Protocol, Verzeichnisdienst
OCSP	Online Certificate Status Protocol, Dienst zur Online Validierung von Zertifikaten
OID	Object Identifier
PED	PIN Entry Device
PIN	Personal Identification Number, Persönliche Nummer zum Aktivieren des Signaturschlüssels
RA	Registration Authority / Registrierungsstelle (Umfasst Swisscom RA, und E-RA und Identitätsprüfstelle)
Re-key	Zertifikaterneuerung mit neuen Schlüsseln
SSCD	Secure Signature Creation Device, Sichere Signaturerstellungseinheit gemäss ETSI TS 101 456
SSL	Secure Socket Layer, Sicherheitsprotokoll
TSP	Time Stamping Profile
TSA	Time-stamping Authority
TAV	Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate

2 Veröffentlichungen und Verantwortung für den Verzeichnisdienst

Die Angaben sind dem CPS [8], 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 der Hierarchie eindeutig referenziert werden können.

Folgende Daten und Nachweise müssen erfasst werden:

Diamant (qualifiziert)	**Namenselement (DN)**	**Erforderlicher Nachweis**
Obligatorisch	CN = <Titel (optional), Vorname, Mittelname (optional), Name *oder* Pseudonym> C = <ISO-Ländercode, zweistellig>	Gemäss vorgelegtem Identifikations-Dokument, siehe auch Kapitel 3.2.2 Gemäss Kapitel 3.1.3 Ländercode des Landes, in dem der Zertifikatsinhaber seinen Wohnsitz hat oder in dem das vorgelegte Identifikations-Dokument des Zertifikatsinhabers ausgestellt wurde.
Optional	<serialNumber> SN = <Nachname> GN = <Vorname> O = <Organisation> OU = <Organisationseinheit> ST = <Kanton> L = <Locality / Ortschaft> STREET = <Postanschrift> E = <Email-Adresse> DC = <Domain Name> pseudonym = <Pseudonym>	Falls erforderlich, z.B. bei Namensgleichheit: zusätzliche Nummer, die die Eindeutigkeit des DN sicherstellt. Gemäss Kapitel 3.2.2 bzw. 3.2.3

Für alle im DN erfassten Attribute müssen Nachweise erbracht werden.

Die Einzelheiten der Attribute sind im CPS [8] Kapitel 3.1.1 festgelegt.

3.1.2 Aussagekraft von Namen

Der DN muss den Zertifikatinhaber eindeutig identifizieren und in einer für Menschen verständlichen Form vorliegen. Bei der Vergabe des DN gelten grundsätzlich die folgenden Regelungen:

- Zertifikate dürfen nur auf einen gemäss den massgeblichen amtlichen Ausweisen zulässigen Namen des Zertifikatinhabers ausgestellt werden.
- Soll der Name der natürlichen Person, welche den Signaturschlüssel kontrolliert, nicht im Zertifikat enthalten sein, muss der Name als Pseudonym gekennzeichnet sein.
- Bei der Vergabe des DN für Pseudonyme 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 weder beleidigende oder anzügliche Inhalt enthalten noch gegen Rechte Dritter (v.a. Namensrecht) oder sonstige Rechtsnormen verstossen.
- Diskriminierungen sind in jeglicher Form 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 [8], Kapitel 3.1.2, festgelegt.

3.1.3 Pseudonymität / Anonymität

In begründeten Ausnahmen kann für eine natürliche Person anstelle des Namens im Zertifikat ein Pseudonym aufgeführt werden. Dieses wird entweder im X.500 Namensfeld "pseudonym" eingefügt oder im CN-Feld des DN eindeutig kenntlich gemacht. Für die Eindeutigkeit von Pseudonymen gelten weiterhin auch die Regelungen in Kapitel 3.1.5. Die Identitätsprüfung erfolgt immer entsprechend den Regelungen in 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 [8], Kapitel 3.1.4, zu entnehmen.

3.1.5 Eindeutigkeit von Namen

Vor der Zertifikatausgabe muss die Korrektheit der Angaben zum DN durch die Registrierungsstelle anhand eines amtlichen Ausweises überprüft werden (vgl. Kapitel 3.2.2). 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.

Nur wenn ein Zertifikatinhaber mehrere Zertifikate mit unterschiedlicher Schlüsselnutzung besitzt, kann ein DN mehrmals vorkommen.

3.1.6 Identifikation, Authentifizierung und Markenschutz

Die Regelung ist im CPS [8], Kapitel 3.1.6, beschrieben.

3.2 Identitätsüberprüfung bei Neuantrag

Please find an English translation of this chapter in the Appendix, chapter 10

3.2.1 Verfahren zur Überprüfung des Besitzes des privaten Schlüssels

Der private Schlüssel wird innerhalb einer sicheren Signaturerstellungseinheit auf der geschützten Infrastruktur von Swisscom erzeugt. Bei der Verwendung eines HSM kann unter Einhaltung der definierten Prozesse der Schlüssel auch direkt im HSM beim Zertifikatsinhaber oder auf der geschützten Infrastruktur von Swisscom erzeugt werden. Die entsprechenden Verfahren werden im CPS [8], Kapitel 3.2.1, beschrieben.

3.2.2 Identifikation und Authentifizierung des Antragstellers

Qualifizierte Zertifikate werden nur an natürliche Personen ausgegeben und Antragsteller können nur natürliche Personen sein. Ein Zertifikatsantrag im Namen einer juristischen Person (Verein, Stiftung, Aktiengesellschaft, Kommanditaktiengesellschaft, Gesellschaft mit beschränkter Haftung, Genossenschaft) oder sonstigen Organisation des Privatrechts (insbesondere Einzelfirma, Kollektivgesellschaft, Kommanditgesellschaft) oder einer öffentlich-rechtlichen Stelle (Behörde, Gericht, Amt, Direktion, öffentlich-rechtliche Anstalt usw.) ist nicht möglich.

Für die Identitätsprüfung des Antragstellers (auch wenn die Person ein Pseudonym verwendet) sind folgende Verfahrensschritte anwendbar:

1. Der Antragsteller muss für die Identitätsprüfung entweder einen gültigen Pass oder eine gültige Schweizer Identitätskarte oder eine für die Einreise in die Schweiz anerkannte, gültige Identitätskarte persönlich vorweisen. Andere Identitätspapiere sind nicht zulässig.
2. Ein RA Mitarbeiter führt die Identitätsprüfung anhand des amtlichen Ausweises (gültiger Pass, gültige Schweizer Identitätskarte oder für die Einreise in die Schweiz anerkannte, gültige Identitätskarte) durch und dokumentiert das Verfahren. Die korrekte Umsetzung der Identifizierung der antragstellenden Person wird mit dem RA-Vertragspartner (E-RA, Identitätsprüfstelle) vertraglich detaillierter geregelt.
3. Für alle im Zertifikat vermerkten Attribute hat der Antragsteller einen Nachweis vorzulegen, beispielsweise mit einer Vollmacht (Art. 7 ZertES [1], Art. 5 Abs. 2 VZertES [2]).

   Bezieht sich das spezifische Attribut auf einen Handelsregistereintrag, so müssen zusätzlich vorgelegt werden:

   a. ein aktueller beglaubigter Handelsregisterauszug (der im Prüfzeitpunkt nicht älter als drei Monate alt sein darf)
   b. die Zustimmungserklärung (im Original, Kopie nicht ausreichend):
      i. bei Einzelunternehmen: von dessen Inhaberin oder Inhaber;
      ii. bei Personengesellschaften: der Gesellschafter;
      iii. bei juristischen Personen: des obersten Leitungs- oder Verwaltungsorgans.

   Attribute, die sich auf die Vertretungsbefugnis einer Organisation (Einzelfirmen, Personengesellschaften, juristische Person, Behörden, usw.) beziehen, werden im Zertifikat

ohne weitere Beschreibung (z.B. des genauen Umfangs der Vertretungsbefugnis oder der Kollektivzeichnungsberechtigung) wie folgt aufgenommen:

- Feld O= <Name der Organisation gemäss Handelsregister oder falls nicht im Handelsregister gemäss sonstigen Nachweisen> und/oder
- Feld OU=<Abteilung / Funktion innerhalb der Organisation>.

Der Eintrag von Attributen erfolgt rein deklaratorisch, der Bestand eines Attributs und dessen möglichen Rechtswirkungen richten sich nach dem anwendbaren Recht (Stellvertretungsrecht, Handelsrecht usw.) und entzieht sich dem Einfluss- und Verantwortungsbereich von Swisscom. Swisscom übernimmt in diesem Zusammenhang einzig Verantwortung für die Überprüfung des Nachweises eines Attributs im Zeitpunkt der Zertifikatsantragsprüfung anhand der hier beschriebenen Nachweise sowie für die Revokationsprozesse. Die auf den Zertifikaten vermerkten Attribute geben nicht alle möglichen rechtlichen Sachverhalte wieder (Zeichnungsberechtigung zu Zweien, Zeichnungsberechtigung nur in Spezialfällen usw.).

Verfügt die beantragende Person bereits über ein gültiges Zertifikat (vgl. Ziffer 4.7 dieser CP für die Gültigkeitsdauer der qualifizierten Zertifikate), kann die Beantragung weiterer Zertifikate für diese Person auch durch die Übersendung eines qualifiziert elektronisch signierten Antrags erfolgen, sofern sich die Identität der Person nicht geändert hat. Voraussetzung für diese Art der Antragstellung ist, dass seit dem Erstantrag des gültigen Zertifikats nicht mehr als drei Jahre vergangen sind und das bei der Identifizierung vorgelegte Ausweisdokument (Pass, oder Schweizer Identitätskarte oder eine für die Einreise in die Schweiz anerkannte Identitätskarte) noch gültig ist.

Die Identität einer Person kann auf Distanz festgestellt werden, sofern eine Konformitätsbewertungsstelle bestätigt hat, dass das verwendete Verfahren zur Personenidentifikation eine gleichwertige Sicherheit zum persönlichen Erscheinen bietet.

Die Personenidentifikation kann mittels einer audiovisueller Kommunikation in Echtzeit erfolgen, wenn das Verfahren den Anforderungen des Geldwäschereigesetzes vom 10. Oktober 1997 [13] entspricht. Die so ausgestellten Zertifikate dürfen nur im Rahmen der Beziehungen zwischen deren Inhaberinnen und Inhabern und den Finanzintermediären, die ihre Identität überprüft haben, verwendet werden.

3.2.3 Nicht überprüfte Informationen

Es werden alle Informationen überprüft, die für die Identitätsprüfung (inkl. Attribute) erforderlich sind (Ziffer 3.2.2). Darüber hinaus werden keine weiteren Informationen überprüft.

3.2.4 Antragsteller mit hohem Risiko

Die Regelungen sind im CPS [8], Kapitel 3.2.5, beschrieben.

3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung

3.3.1 Routinemässige Zertifikaterneuerung (re-key)

Sofern alle hinterlegten Dokumente für die Identifikation noch aktuell und gültig sind und keine zusätzlichen Attribute im neuen Zertifikat aufgenommen werden sollen, sind keine zusätzlichen

Massnahmen zur Identifikation des Antragsstellers nötig. Voraussetzung für diese Art der Antragstellung ist, dass die Registrierungsstelle deren Identität innerhalb der letzten sechs Jahre nach Kapitel 3.2.2 festgestellt hat.

Für alle anderen Fälle (insbesondere, wenn die Aufnahme oder Beibehaltung von Attributen gewünscht ist), 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

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

4 Betriebsanforderungen an den Zertifikats Lebenszyklus

4.1 Zertifikatsantrag

4.1.1 Wer kann ein Zertifikat beantragen

Folgende Personen können ein „qualifiziertes“ Zertifikat beantragen: natürliche Personen.

4.1.2 Registrierungsprozess

Ein Zertifikat kann durch Swisscom erst erzeugt werden, wenn der Registrierungsprozess bei einem RA-Vertragspartner erfolgreich abgeschlossen wurde. Die Dokumentation des Registrierungs-prozesses beinhaltet zumindest:

- signierter Zertifikatantrag (Original);
- Farbkopie vom Ausweisdokument (gültiger Pass oder gültige Schweizer Identitätskarte oder für die Einreise in die Schweiz anerkannte, gültige Identitätskarte);
- Bestätigung des Antragstellers eines Zertifikats, den Kundenvertrag bzw. Bestätigung des Antragstellers, die Nutzungsbestimmungen für qualifizierte Zertifikate (Klasse „Diamant“) gelesen, verstanden und angenommen zu haben (Original);
- Falls Vermerk von Attributen beantragt: Originaldokumente betreffend Attribute, insbesondere Vertretungsvollmachten und gegebenenfalls beglaubigter Handelsregisterauszug und schriftliche Zustimmungserklärung;
- 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 Zertifikatsanträgen

4.2.1 Durchführung der Identifikation und Authentifizierung

Die zuständige Registrierungsstelle von Swisscom oder des RA-Vertragspartners führt die Identifikation und Authentifizierung eines Antragstellers nach den im Kapitel 3.2 beschriebenen Verfahren durch.

4.2.2 Annahme oder Abweisung von Zertifikatanträgen

Zertifikatanträge sind an die RA-Vertragspartner 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 [8], 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 TAV [3], Art. 2.2.3 eingesetzt wird,
- durch Swisscom ein qualifiziertes Zertifikat der Klasse „Diamant“ ausgestellt,
- das Zertifikat dem Antragsteller ausgehändigt 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

a) *Der Zertifikatsinhaber hält Zertifikat und privaten Schlüssel auf eigenem SSCD:*

   Nach der Zertifikatausstellung wird dem Antragsteller das ausgestellte Zertifikat zusammen mit der sicheren Signaturerstellungseinheit in geeigneter Weise übermittelt. Nimmt der Antragsteller eines Zertifikats die sichere Signaturerstellungseinheit nicht persönlich entgegen, so ist die Übermittlung angemessen zu schützen. Die Verfahren sind dem CPS [8], Kapitel 4.3, zu entnehmen.

b) *Die privaten Schlüssel verbleiben in der sicheren Umgebung der Swisscom:*

Der Antragsteller wird nicht über die Zertifikatsausstellung informiert.

4.3.3 Benachrichtigung weiterer Instanzen

Eine Benachrichtigung weiterer Instanzen ist nicht vorgesehen.

4.4 Zertifikatakzeptanz

Es gelten die Regelungen in Kapitel 4.4 der CPS [8].

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,
- das Zertifikat ausschliesslich in Übereinstimmung mit dieser CP eingesetzt wird.

Der Zertifikatsinhaber mit eigenem SSCD (z.B. HSM) versichert zudem, dass

- 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 abhanden kommt, gestohlen wurde oder sonst möglicherweise Dritten zur Kenntnis gelangt ist (Kompromittierung).

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, muss

- 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 basierend auf dem alten Schlüssel (certificate renewal) wird durch Swisscom für qualifizierte Zertifikate der Klasse „Diamant“ 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. Die Lebensdauer des Zertifikates beträgt maximal 3 Jahre.

Bei der Verwendung eines HSM wird im HSM ein neues Schlüsselpaar erzeugt.

Es werden die Schlüssellänge und der Algorithmus verwendet, welche zu dem jeweiligen Zeitpunkt aktuell und gemäss geltender CPS [8] einzusetzen sind. Der Zertifikatinhaber hat zu bestätigen, dass die im Zertifikat enthaltenen Informationen unverändert bleiben und die anlässlich der Zertifikatsausstellung vorgelegten Ausweise und 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 beantragt werden, wenn:

- die Gültigkeit des Zertifikats abläuft;
- 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 qualifizierten Zertifikaten der Klasse „Diamant“ 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).

4.9 Ungültigerklärung und Suspendierung von Zertifikaten

In diesem Abschnitt werden die Umstände erläutert, unter denen ein Zertifikat nach Art. 11 ZertES [1] 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 Aktualisierungs-Intervall der CRL (siehe Kapitel 4.9.7), wird keine Ungültigerklärung angeboten.

4.9.1 Gründe für eine Ungültigerklärung

Zertifikate müssen von der zuständigen RA oder von Swisscom 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 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.

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 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 [8], Kapitel 4.9, zu entnehmen. Voraussetzung für die Akzeptanz einer Ungültigerklärung des Zertifikats ist eine erfolgreiche Identifizierung und Authentifizierung des Zertifikatinhabers entsprechend Ziffer 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 Autorisierungsinformation bzw. Identitätsprüfung nach Ziffer 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 angerufen.
- 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.
- Ein Widerrufsantrag kann auch über das Web-Portal der Swisscom Digital Certificate Services gestellt werden. Zur Verifikation der Identität wird der Zertifikatsinhaber angerufen.

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 für eine Ungültigerklärung gemäss Kapitel 4.9.1 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

Die CRL wird alle 2 Stunden nachgeführt.

4.9.8 Maximale Latenzzeit für CRL

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

4.9.9 Verfügbarkeit von Online-Ungültigkeits/Status-Überprüfungsverfahren

Swisscom Digital Certificate Services bietet mehrere Online-Verfahren an, mit dem die Gültigkeit eines Zertifikats überprüft werden kann. Es sind dabei alle Zertifikate erfasst, die von der CA 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 [9] 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 [8] 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 qualifizierten Zertifikaten der Zertifikatsklasse „Diamant“ wird nicht angeboten.

4.10 Dienst zur Statusabfrage von Zertifikaten

Die Details zum Verfahren, Verfügbarkeit und Merkmalen sind dem Kapitel 4.10 der CPS [8] 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) ist für qualifizierte Signaturschlüssel gemäss ZertES [1] nicht erlaubt und wird nicht angeboten.

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

Bei der Verwendung eines HSM darf der Signaturschlüssel für ein Backup in geeigneter Weise exportiert werden, sofern der Signaturschlüssel gleichwertig geschützt ist wie im HSM, und ausgeschlossen werden kann, dass der Signaturschlüssel ausserhalb des HSM genutzt werden kann.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen

Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen sind dem CPS [8], Kapitel 5, zu entnehmen.

6 Technische Sicherheitsmassnahmen

Technische Sicherheitsmassnahmen sind dem CPS [8], Kapitel 6, zu entnehmen.

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

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

7.1 Zertifikatsprofil

Ein von Swisscom Digital Certificate Services ausgegebenes qualifiziertes Zertifikat der Klasse „Diamant“ umfasst folgende, im X.509 v3 Standard definierte und gemäss TAV [3] verlangten Pflichtfelder:

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

Die Details des Zertifikatsprofiles sind dem Addendum zum CPS [9] Kapitel 2 zu entnehmen.

7.1.1 Zertifikaterweiterungen

Es sind folgende, im X.509 v3 Standard definierten und gemäss TAV [3] verlangten Erweiterungen vorhanden:

- Digitale Signatur der CA (nicht kritisch)
- Verwendungszweck des Zertifikates (kritisch)
- Zertifizierungsrichtlinie (nicht kritisch)
- CRL Distribution Point (nicht kritisch)
- Zugangspunkt zum Zertifikat der CA (nicht kritisch)
- Hinweis: qualifiziertes Zertifikat (nicht kritisch)
- Hinweis: private key in SSCD (nicht kritisch)
- Hinweis: Grenzwert einer Transaktion (nicht kritisch).

8 Konformitätsüberprüfung (Compliance Audit) und andere Assessments

Swisscom und die RA-Vertragspartner, welche qualifizierte Zertifikate ausstellen, sind verpflichtet, alle ihre Abläufe dieser CP und dem CPS entsprechend auszugestalten.

Swisscom ist eine anerkannte Anbieterin von Zertifizierungsdiensten im Sinne des ZertES [1]. Die Erfüllung der Voraussetzungen für die Anerkennung als Anbieterin von Zertifizierungsdiensten wurde gemäss ZertES [1] Abschnitt 2 durch eine durch die schweizerische Akkreditierungsstelle akkreditierte Anerkennungsstelle überprüft. Siehe dazu auch https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas/pki.html

8.1 Intervall und Umstände der Überprüfung

Nach dem erstmaligen Audit führt die Anerkennungsstelle regelmässig eine Rezertifizierung durch. Zusätzlich verpflichtet sich Swisscom, 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. 9 Abs. 6 ZertES [1]).

8.2 Identität und Qualifikation der Überprüferin

Die regelmässig wiederkehrende Konformitätsprüfung wird durch eine von Swisscom unabhängige Unternehmung, durchgeführt. Nur durch die Schweizerische Akkreditierungsstelle (SAS) akkreditierte Firmen dürfen diese Prüfung durchführen. Die Liste der akkreditierten Stellen ist auf der Internetseite der SAS in der Rubrik „Akkreditierte Stellen“ abrufbar (https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas/pki.html).

Die interne 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. Externe und interne 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.

8.4 Überprüfte Bereiche

Die von einer Überprüfung betroffenen Bereiche werden jeweils durch die externen 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 der zuständigen Anerkennungsstelle und der überprüften Zertifizierungs- bzw. Registrierungsstelle zeitnah behoben. Schwerwiegende Mängel mit hohem Risiko innert 2 Wochen, alle anderen innerhalb von 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

9.1 Gebühren

Die Regelungen sind dem CPS [8], Kapitel 9.1 zu entnehmen.

9.2 Finanzielle Verantwortung

Die Regelungen sind dem CPS [8], Kapitel 9.2 zu entnehmen.

9.3 Schutz von Personendaten (Datenschutz)

Die Regelungen sind dem CPS [8], Kapitel 9.3 zu entnehmen.

9.4 Immaterialgüterrechte

Die Regelungen sind dem CPS [8], Kapitel 9.4 zu entnehmen.

9.5 Zusicherung und Gewährleistung

Die Regelungen sind dem CPS [8], Kapitel 9.5 zu entnehmen.

9.6 Ausschluss der Gewährleistung

Entfällt

9.7 Haftung von Swisscom (Schweiz) AG

Swisscom haftet der Inhaberin oder dem Inhaber des Signaturschlüssels und Drittpersonen, die sich auf ein gültiges Zertifikat verlassen, für Schäden, die diese erleiden, weil Swisscom ihren Pflichten nicht nachgekommen ist. Swisscom trägt die Beweislast dafür, den Pflichten als Zertifizierungsstelle nachgekommen zu sein.

Swisscom haftet nicht für Schäden, die sich aus der Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung im Zertifikat ergeben.

Swisscom haftet nicht, wenn die Erbringung der Leistung auf Grund höherer Gewalt zeitweise unterbrochen, ganz oder teilweise beschränkt oder unmöglich ist. Als höhere Gewalt gelten insbesondere Naturereignisse von besonderer Intensität (Lawinen, Überschwemmungen, Erdrutsche usw.), kriegerische Ereignisse, Aufruhr, unvorhersehbare behördliche Restriktionen usw..

Kann Swisscom ihren vertraglichen Verpflichtungen infolge eines derartigen Ereignisses nicht nachkommen, wird die Vertragserfüllung oder der Termin für die Vertragserfüllung dem eingetretenen Ereignis entsprechend hinausgeschoben. Swisscom haftet nicht für allfällige Schäden, die dem Kunden durch das Herausschieben der Vertragserfüllung entstehen.

In allen anderen Fällen haftet Swisscom wie folgt:

- Bei Vertragsverletzungen haftet Swisscom für den nachgewiesenen Schaden, sofern sie nicht beweist, dass sie kein Verschulden trifft.
- Für absichtlich und grobfahrlässig verursachte Schäden haftet Swisscom unbegrenzt.
- Bei leichter Fahrlässigkeit haftet Swisscom für Personenschäden unbegrenzt, für Sachschäden bis zu einem Betrag von CHF 500'000 je Schadenereignis und für Vermögensschäden höchstens bis zu einem Betrag von CHF 50'000 je Schadenereignis.

In keinem Fall haftet Swisscom für Folgeschäden, insbesondere entgangenen Gewinn oder Daten- oder Reputationsverluste.

9.8 Haftung des Zertifikatinhabers

Die Regelungen sind dem CPS [8], Kapitel 9.8 zu entnehmen.

9.9 Inkrafttreten und Aufhebung

Die Regelungen sind dem CPS [8], Kapitel 9.9 zu entnehmen.

9.10 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

Die Regelungen sind dem CPS [8], Kapitel 9.10 zu entnehmen.

9.11 Änderungen der Zertifizierungsrichtlinien

Die Regelungen sind dem CPS [8], Kapitel 9.11 zu entnehmen.

9.12 Konfliktbeilegung

Die Regelungen sind dem CPS [8], Kapitel 9.12 zu entnehmen.

9.13 Geltendes Recht und Gerichtsstand

Die Regelungen sind dem CPS [8], Kapitel 9.13 zu entnehmen.

9.14 Konformität mit dem geltenden Recht

Die Regelungen sind dem CPS [8], Kapitel 9.14 zu entnehmen.

9.15 Weitere Bestimmungen

Die Regelungen sind dem CPS [8], Kapitel 9.15 zu entnehmen.

10 Appendix

English translation of the identification and authentication processes, chapter 3.2

„3.2 Initial Identity Verification"

„3.2.1 Method for proving Possession of the Private Key"

The private key is generated within a secure signature creation device within the protected infrastructure of Swisscom or a contractor. When using an HSM in compliance with the defined processes, the key can also be generated directly on the HSM of the certificate holder or on the servers of the All-in Signing Service. These procedures are described in the CPS [8], section 3.2.1,

„3.2.2 Identification and authentication of the applicant"

Qualified certificates are issued only to natural persons and applicants may be only natural persons. A certificate application on behalf of a legal entity (association, foundation, corporation, partnership limited, limited liability company, association) or any other organization under private law (in particular, sole proprietorship, general partnership, limited partnership) or a public body (authority, court, Office, Directorate, a public law institution, etc.) is not possible.

For identity verification of the applicant (even if the person used a pseudonym), the following steps apply:

1. For identity verification, the applicant must personally present either a valid passport or a valid Swiss ID card or a valid identity card authorizing entry into Switzerland. Other identity papers are not allowed.
2. An RA employee performs the identity verification using the official identity card (valid passport, valid Swiss ID card or a valid identity card authorizing entry into Switzerland) and documents the process. The correct implementation of the identification of the applicant is covered in more detail by a contract with the RA partners (E-RA / IVA).
3. For all the attributes mentioned in the certificate, the applicant shall provide proof, for example with a power of attorney (Art. 8 ZertES [1], Art. 5 para. 2 VZertES [2]).

   Refers a specific attribute to a commercial register entry, the following documents must be submitted in addition:

   a. a current certified commercial register (which may not be older than three months at the time of testing)
   b. the consent solicitation (in original, a copy is not sufficient):
      i. for individual enterprises: its owner or holder;
      ii. for partnerships: the shareholder;
      iii. for legal entities: the top management or administrative organ

   Attributes that relate to the power of representation of an organization (sole proprietorships, partnerships, legal persons, government agencies, etc.) will be included in the certificate without further description (e.g. the precise extent of the right of representation or collective signing) as follows:

   - O field = <name of the organization in the commercial register or, if not in the commercial register pursuant to other evidence>

   and / or

   - OU field = <department / function within the organization>.

The entry of attributes is purely declaratory; the characteristics of an attribute and its possible legal consequences shall be governed by the applicable law (substitution law, commercial law, etc.) and is outside of the influence and responsibility of Swisscom. In this context Swisscom takes over only the responsibility for checking of the proof of an attribute at the time the certificate application is being tested based on evidence described here and for the revocation processes. The attributes mentioned on the certificates do not describe all possible legal situations (signing jointly with a second person, signing only in special cases, etc.).

If the applicant already has a valid certificate (cf. number 4. 7 CP for the period of validity of qualified certificates), the application for additional certificates for this person also can be made by sending an electronically qualifiedly signed application provided that the identity of the person hasn't changed. A prerequisite for this type of application is that since the initial application of the valid certificate no more than three years have passed and that the initially provided identity document (passport or Swiss identity card or identity card authorizing entry into Switzerland) is still valid.

The identity of a person can be determined at a distance, provided that a conformity assessment body has confirmed that the method used for personal identification provides an equivalent security for personal appearance.

The identification of persons can be carried out in real time by means of audiovisual communication if the procedure complies with the requirements of the Money Laundering Act of 10 October 1997 [13]. The certificates issued in this way may only be used in the context of the relations between their holders and the financial intermediaries who have verified their identity.

„3.2.3 Unverified Information"

All information that are necessary for the identity verification (see section 3.2.2) will be checked (incl. attributes). Beyond these, no further information will be verified.

„3.2.4 Applicants with a high risk"

The regulations are described in the CPS, chapter 3.2.5.