Swisscom Digital Certificate Services

Certificate Policy (CP)

Zertifikatsklasse „Smaragd“ (fortgeschritten)

Zusammenfassung	Certificate Policy für fortgeschrittene Zertifikate der Swisscom Digital Certificate Services, einer Dienstleistung der Swisscom (Schweiz) AG zur Ausgabe von digitalen Zertifikaten für Personen, Dienste und Geräte.
Name	007_cp_smaragd_2_16_756_1_83_v2.3.doc
Version	2.3
Klassifizierung	Nicht klassifiziert
OID der CP	2.16.756.1.83.6 (Smaragd CA 1) 2.16.756.1.83.17.0 (Smaragd CA 2)
Zugehöriges CPS	CPS Swisscom Digital Certificate Services OID: 2.16.756.1.83.2.1
Name der CA	Swisscom Smaragd CA 1 (OID 2.16.756.1.83.6) Swisscom Smaragd CA 2 (OID 2.16.756.1.83.17)
Owner der CA	Swisscom (Schweiz) AG
Sprachversion:	Deutsch (Rechtlich verbindliche Originalversion) *English translations of selected sections in the Appendix (original version in German is legally binding)*
Beginn der CP-Konformitätsprüfung:	4. April 2006 (Smaragd CA 1) 1. Januar 2011 (Smaragd CA 2)
Freigabe des Dokuments	Governance Board der Swisscom Digital Certificate Services

Änderungskontrolle

Version	Datum	Ausführende Stelle	Bemerkungen/Art der Änderung
1.0	21. Juni 2010	Governance Board	Freigegeben
2.1	08.07.2011	Governance Board	Freigegeben
2.2	03.11.2011	Projekt Team	Ergänzungen SHA-256, Unterscheidung CA 1 und CA 2
2.2	21.11.2011	Governance Board	Freigabe
2.2a	16.10.2012	Projekt Team	Übersetzungen in English / Translations
2.2b	07.11.2012	Projekt Team	Update CAB Referenz
2.3	27.07.2014	Kerstin Wagner	Review und Update
2.3	25.09.2014	Governance Board	Freigabe

Referenzierte Dokumente:

Referenz	Bezeichnung
[1]	SR 943.03, ZertES: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur)
[2]	SR 943.032, VZertES: Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (Verordnung über die elektronische Signatur)
[3]	SR 943.032.1, TAV: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur
[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]	IETF RFC 5280: „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“
[7]	IETF RFC 2560:„X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP“
[8]	CPS Swisscom Digital Certificate Services, OID 2.16.756.1.83.2.1
[9]	IETF RFC1034: Domain Names – Concepts and Facilities
[10]	IETF RFC791:- Internet Protocol, Version 4 (IPv4) Specification
[11]	Richtlinien des CA/Browser-Forums für die Ausstellung und Verwaltung von Extended-Validation-Zertifikaten („Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“, https://www.cabforum.org/forum.html)
[12]	Addendum zum CPS [8]: Profile der Zertifikate, Widerrufslisten und Online Statusabfragen

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument beschreibt die Certificate Policy (Zertifizierungspolitik, nachfolgend CP) von Swisscom Digital Certificate Services, einer Dienstleistung der Swisscom (Schweiz) AG [nachfolgend Swisscom] zur Ausgabe von fortgeschrittenen Zertifikaten nach schweizerischem Signaturgesetz ZertES [1] und den referenzierten technischen und administrativen Ausführungsbestimmungen TAV[3] und VZertES [2].

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

Ein „Smaragd“ Zertifikat ist eine elektronische Bescheinigung, mit der ein öffentlicher kryptografischer Schlüssel eines Datenverarbeitungssystems (Device/Server-Komponente) zugeordnet und mit der die Identität der Person oder Organisation bestätigt wird. Ein Smaragd Zertifikat stellt also eine Verbindung zwischen einer Person oder Organisation und einem kryptografischen Schlüssel eines Datenverarbeitungssystems her.

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 Swisscom Digital Certificate Services Certification Practice Statement (nachfolgend CPS) entnommen werden.

Diese CP bezieht sich auf die Zertifikatklasse Smaragd (Soft-Zertifikat), einem„fortgeschrittenen digitalen Zertifikat“, welches den Anforderungen des schweizerischen Signaturgesetzes entspricht. Für alle Zertifikate, die dieser CP entsprechen, ist der Objekt Identifikator gemäss X.509 [OID] dieser CP im Zertifikat vermerkt. Somit wird die CP an das Zertifikat einer bestimmten Klasse gebunden.

Die vorliegenende CP bezieht sich auf zwei unterschiedliche CA Generationen. Die mit der Endung CA 1 bezeichnete erste Generation verwendet durchwegs SHA-1 als Hash-Algorithmus, während die mit CA 2 identifizierte CA Hierarchie für alle Zertifikate SHA-256 als Hash-Algorithmus einsetzt. Die Nummerierung wird innerhalb einer CA Hierarchie konstant gehalten, d.h. alle CA 1 Issuing CAs sind unterhalb der CA 1 Root ausgestellt, während alle Issuing CA 2 von der Root CA 2 signiert sind.
Falls nicht näher bezeichnet, beziehen sich die Angaben in diesem Dokument immer auf beide CA Generationen.

1.1 Überblick

Diese fortgeschrittene CP wurde von Swisscom zu folgendem Zweck erstellt:

- Erfüllung der Anforderungen an einen Certification Service Provider (nachfolgend CSP) von fortgeschrittenen Zertifikaten gemäss ZertES [1]
- Beschreibung der Dienstleistungen, Rollen, Einschränkungen und Verpflichtungen bei der Verwendung von fortgeschrittene Zertifikaten der Swisscom Digital Certificate Services

- Sicherstellung der Interoperabilität bei der Benutzung fortgeschrittener Zertifikate der Swisscom Digital Certificate Services.
- Erfüllung der Anforderungen an CSP, die EV-Zertifikate ausstellen, gemäss den Vorgaben des CA/Browser-Forums [11];

  Swisscom Digital Certificate Services befolgt die aktuelle Version der Grundanforderungen, die auf http://www.cabforum.org veröffentlicht sind, für die Ausgabe und Verwaltung von vertrauenswürdigen öffentlichen Zertifikaten. Im Falle eines Widerspruchs zwischen diesem Dokument und den Grundanforderungen, erhalten die Grundanforderungen Vorrang vor diesem Dokument.

  English Translation see 10.1(„1.1 Overview").

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

- SR 943.032.1 [3]
- ETSI TS 101 456 [5]

Um die internationale Zusammenarbeit mit anderen Zertifizierungsstellen zu ermöglichen, wird ferner eine englische Übersetzung der CP veröffentlicht; 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 Smaragd
- Version: 2.3
- Object Identifier (OID) für diese CP:
  - Smaragd CA 1: 2.16.756.1.83.6
  - Smaragd CA 2: 2.16.7556.1.83.17.0

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		zur Bezeichnung der Namen von Organisationen (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 Off-Line Root Certification Authority (nachfolgend CA) sowie eine der Root CA untergeordnete CA für fortgeschrittene Zertifikate („Smaragd“). 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 Zertifizierungsstellen der Swisscom Digital Certificate Services aus. Die Smaragd-CA2 stellt nur Zertifikate an Datenverarbeitungssysteme aus, die allerdings vertreten werden von natürlichen Personen, welche wiederum Vertreter einer juristischen Person oder Organisation sein können.

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

1.3.2 Registrierungsstellen – Registration Authorities (RA)

Das Geschäftsmodell von Swisscom basiert auf einem Registration Authorities (nachfolgend RA) Vertragspartner-Modell. Dabei übernehmen Vertragspartner von Swisscom die RA-Funktion.

Das Geschäftsmodell von Swisscom unterscheidet drei Typen von RA:

- Swisscom-RA: Zur Ausgabe von Zertifikaten für den Eigengebrauch und der nachgelagerten RA’s (E-RA)
- Enterprise-RA: (Enterprise Registration Authority, nachfolgend E-RA) ist ein RA-Partner, der in der Lage ist, SSCD und Zertifikate sowie nicht SSCD basierte Zertifikate selber zu erstellen und auszugeben.
- TPS: (Trusted Point of Sale) ist ein RA-Partner, der als Registrierungsstelle Zertifikatsanträge entgegennimmt und die Angaben überprüft. Die nicht SSCD basierte Zertifikate der Zertifikatsklassen „Smaragd“ werden von einer E-RA oder einer zentralen Verteilstelle personalisiert und verteilt.

Wird von einer RA gesprochen, umfasst dies die RA, welche durch Swisscom betrieben werden und die E-RA/TPS der Vertragspartner. Mit dem RA-Vertragspartner Modell soll sichergestellt werden, dass:

- Die angebotenen Zertifikate optimal in die entsprechenden Anwendungen des Partners eingebunden sind
- Der Benutzer auf möglichst einfache Weise zu seinem Zertifikat kommt
- Zertifikate von Swisscom Digital Certificate Services bei mehreren Dienstanbietern eingesetzt werden können

1.3.3 Zertifikatinhaber (Subscriber)

Fortgeschrittene Zertifikate der Klasse „Smaragd“werden an natürliche Personen oder Organisationen als Vertretung eines Datenverarbeitungssystems (Server/Device) vergeben, soweit dies den Nutzungsbestimmungen von Swisscom oder des RA-Vertragspartners entspricht.

1.3.4 Zertifikatprüfer (Relying Parties)

Unter Zertifikatprüfern sind natürliche Personen oder Organisationen zu verstehen, die unter Nutzung eines von Swisscom Digital Certificate Services ausgestellten Zertifikats die Identität eines Zertifikatinhabers überprüfen oder von diesem Informationen entgegennehmen oder diesem Informationen zukommen lassen. Ein Zertifikatprüfer kann – muss aber nicht – Teilnehmer der Swisscom Digital Certificate Services sein.

1.3.5 Weitere Teilnehmer

Weitere Teilnehmer können natürliche oder juristische Personen sein, die in den Zertifizierungs- oder Registrierungsprozess als Dienstleister eingebunden sind. Bei Dienstleistern, die im Namen und Auftrag eines Zertifikatinhabers oder Prüfers tätig werden, liegt die Verantwortung bei dem beauftragenden Zertifikatinhaber.

Der Abschluss von Dienstleistungsabkommen mit einem Dienstleister oder die Entgegennahme und Akzeptanz von Leistungen eines Dienstleister, der im eigenen Namen handelt, kann ausschliesslich durch die Service Leitung der Swisscom Digital Certificate Services vorgenommen werden.

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, Authentisierung und Verschlüsselung verwendet werden. Zusätzlich können die Zertifikatsangaben für die Abfrage von Statusinformationen der ungültig erklärten Zertifikate beim CSP verwendet werden.

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 Digital Certificate Services definiert werden. Die verwendeten Anwendungsprogramme müssen dazu den Sicherheitsanforderungen geeignet Rechnung tragen. Eine Installation von Anwendungsprogrammen durch Swisscom Digital Certificate Services sowie durch deren Vertragspartner findet nicht statt.

1.4.2 Untersagte Zertifikatnutzung

Grundsätzlich ist das Signieren, Verschlüsseln und Authentisieren mit einem fortgeschrittenen Zertifikat erlaubt. Alle anderen Nutzungen sind untersagt.

1.5 Verwaltung der Richtlinien

Herausgeberin des Dokumentenframeworks ist:

Swisscom (Schweiz) AG
Digital Certificate Services
Müllerstrasse 16
8004 Zürich

Es gilt ein formelles Genehmigungsverfahren gemäss CPS [8] 1.5.4.

1.6 Schlüsselwörter und Begriffe

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

1.7 Abkürzungen

Begriff	*Erklärung*
AIS	All-in Signing Service
BCP	Business Continuity Plans
CA	Certification Authority
CAB	CA/Browser Forum
CN	Common Name, als Teil des DN
CP	Certificate Policy, Zertifizierungsrichtlinien
CPS	Certification Practice Statement, Aussage über die Zertifizierungspraxen
CSP	Certification Service Provider
CRL	Certificate Revocation List
CN	Common Name, als Teil des DN
DN	Distinguished Name gemäss RFC 3739
EE	End Entity
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
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
PED	PIN Entry Device
PIN	Personal Identification Number, Persönliche Nummer zum Aktivieren des Signaturschlüssels
RA	Registration Authority / Registrierungsstelle (Umfasst RA der Swisscom und E-RA/TPS)
Re-Key	Zertifikaterneuerung
SSCD	Sichere Signaturerstellungseinheit, Secure Signature Creation Device gemäss ETSI TS 101 456
SSL	Secure Socket Layer, Sicherheitsprotokoll
TSP	Time Stamping Profile
TPS	Trusted Point of Sales
TSA	Time-stamping Authorities
TAV	Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur

	(Verordnung über die elektronische Signatur, VZertES) vom 3. Dezember 2004
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur vom 19. Dezember 2003

2 Veröffentlichungen und Verantwortung für den Verzeichnisdienst

2.1 Verzeichnisdienst

Swisscom Digital Certificate Services als CSP stellt sicher, dass Informationen zur Überprüfung der Gültigkeit der von ihr ausgegebenen Zertifikate kostenlos über ein Web-Interface sowie eine LDAP Abfrage bereitgestellt werden (Art. 11 Abs. 1 ZertES[1]). Zusätzliche Statusdienste sind der CPS [8] Kapitel 2.1 zu entnehmen.

Ungültige Zertifikate werden in einer Liste der für ungültig erklärten Zertifikate (nachfolgend CRL) geführt. Die CRL wird alle 2 Stunden aktualisiert.

Details sind dem CPS [8] Kapitel 2.2 und 2.3 zu entnehmen.

2.2 Veröffentlichung von Informationen

Swisscom Digital Certificate Services als CSP veröffentlicht folgende Informationen:

- Das Wurzelzertifikat der Swisscom Digital Certificate Services
- Zertifikate der nächsten CA-Stufe (Level 1)
- Diese CP und zugehöriges CPS [8].

Darüber hinaus werden Informationen über die Swisscom Digital Certificate Services, über die korrekte Anwendung von Kryptographie und die Verwendung von Zertifikaten den Zertifikatinhabern zur Verfügung gestellt. Details der Bezugsadressen dieser Informationen und ggf. weiterer Dienstleistungen sind dem CPS [8] Kapitel 2.2 zu entnehmen.

2.3 Aktualisierung der Informationen

Swisscom Digital Certificate Services aktualisiert die Informationen zur Überprüfung der Gültigkeit von Zertifikaten in regelmässigen Abständen. Der Abstand zwischen zwei Aktualisierungen beträgt 2 Stunden. Einzelheiten sind dem CPS [8] Kapitel 2.3 zu entnehmen.

2.4 Zugang zu den Informationsdiensten

Der lesende Zugriff auf alle in den Abschnitten 2.1 und 2.2 aufgeführten Informationen unterliegt keiner Zugangskontrolle. Es werden keine Massenabfragen oder „Wildcard-Abfragen“ unterstützt. Schreibender Zugriff auf diese Informationen darf nur berechtigten Personen gewährt werden. Details sind dem CPS [8] Kapitel 2.4 zu entnehmen.

3 Identifizierung und Authentifizierung

3.1 Namen

3.1.1 Namensform

Es wird eine einheitliche Namenshierarchie verwendet. Alle innerhalb der Swisscom Digital Certificate Services ausgestellten Zertifikate haben eindeutige Namen (Distinguished Name, nachfolgend DN) entsprechend der Normenserie X.500. Ein DN enthält eine Folge von eindeutig kennzeichnenden Namensattributen, durch die alle Teilnehmer einer Hierarchie referenziert werden können.

Die Einzelheiten für die spezifischen Namensformen 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 Namensvergabe gelten grundsätzlich die folgenden Regelungen:

- Zertifikate dürfen nur auf eine zulässige Datenverarbeitungssystem Bezeichnung des Zertifikatinhabers ausgestellt werden.
- Bei der Vergabe von Bezeichnungen für technische Datenverarbeitungssysteme muss eine Verwechslung mit natürlichen und juristischen Personen, Bezeichnungen von Organisationseinheiten oder Dritt Systemen ausgeschlossen werden. Es dürfen DNS-Namen und IP-Adressen verwendet werden. Es dürfen keine innerhalb der Swisscom Digital Certificate Services benutzten Syntaxelemente verwendet werden.

  Eine technische Bezeichnung darf keinen beleidigenden oder anzüglichen Inhalt enthalten oder gegen Rechtsnormen oder Rechte Dritter (v.a. Namensrecht) 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] unter 3.1.2 festgelegt.

Als „Distinguished Names" [6] für Datenverarbeitungssysteme sind ausschliesslich Internet-Domainnamen bzw. öffentliche FQDN, gemäss RFC Inhalte zugelassen. Als „GeneralName" [6] für Datenverarbeitungssysteme sind ausschliesslich Internet-Domainnamen bzw. öffentliche FQDN, gemäss RFC1034 [9] dNSName bzw. RFC791 [10] iPAddress Inhalte zugelassen.

3.1.3 Pseudonymität / Anonymität

Zertifikate werden ausschliesslich an juristische Personen vergeben, die ihre Identität gemäss der beschriebenen Vorgehensweise beweisen können. Der Name der natürlichen Person, die über den privaten Schlüssel verfügt, muss im Zertifikat nicht genannt werden, Swisscom aber vorliegen.

Die Angaben im CN-Feld des DN müssen eine eindeutige und zuverlässige Identifikation der Organisation oder juristischen Person erlauben. Einzelheiten regelt das CPS [8] Kapitel 3.1.3.

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 amtlicher Ausweise überprüft und sichergestellt werden. Die Eindeutigkeit des angegebenen Namens muss von der zuständigen RA überprüft werden. Der DN eines Zertifikatinhabers muss eindeutig sein und darf nicht an unterschiedliche Zertifikatinhaber vergeben werden. Nur wenn ein Zertifikatinhaber mehrere Zertifikate mit unterschiedlicher Schlüsselnutzung besitzt, kann ein DN mehrmals vorkommen. Seriennummern in Bezug zu der ausstellenden CA sind jedoch uneingeschränkt eindeutig.

3.1.6 Erkennung, Authentifizierung und Funktion von Warenzeichen

Es liegt in der Verantwortung des Zertifikatinhabers, dass die Namenswahl keine Warenzeichen, Markenrechte usw. verletzt. Der CSP ist nicht verpflichtet, solche Rechte zu überprüfen. Allein der Zertifikatinhaber ist für solche Überprüfungen verantwortlich. Falls der CSP über eine Verletzung solcher Rechte informiert wird, wird das Zertifikat ungültig erklärt.

3.2 Identitätsüberprüfung bei Neuantrag

English Translation see 10.2 „3.2 Identity verification for new application"

3.2.1 Verfahren zur Überprüfung des Besitzes des privaten Schlüssels

Das Schlüsselpaar wird innerhalb der Kunden Infrastruktur erstellt. Der öffentliche Schlüssel wird in einer sicheren Signaturerstellungseinheit auf der geschützten Infrastruktur des CSP signiert. Die Sicherung des privaten Schlüssels obliegt dem Zertifikats Inhabers. Die entsprechenden Verfahren werden im CPS [8] Kapitel 3.2.1 beschrieben.

3.2.2 Authentifizierung einer juristischen Person

Juristische Personen werden über einen offiziellen Vertreter identifiziert. D.h. die Person welche ein Smaragd Zertifikat für eine Organisation bzw. juristische Person beantragt, muss einen Nachweis in Form einer gültigen Vollmacht und oder einer Beglaubigung der RA vorlegen, dass Sie im Auftrag der juristischen Person bzw. Organisation handelt. Des Weiteren gelten die Ausführungen gemäss 3.2.3.

3.2.3 Authentifizierung einer natürlichen Person

Für die Identitätsprüfung einer natürlichen Person oder die juristische Person, für die der Antragsteller eine Rolle wahrnimmt, für ein fortgeschrittenes Zertifikat sind folgende Verfahrensschritte anwendbar:

1. Der Antragsteller eines Zertifikats sendet der RA eines oder mehrere seine Identität bestätigende Dokumente.

2. Ein RA Mitarbeiter führt die Identitätsprüfung anhand der durch den Antragsteller zur Verfügung gestellten Dokumente und dokumentiert das Verfahren.
3. Für alle im Zertifikat des Datenverarbeitungssystems vermerkten Attribute haben Nachweise zu erfolgen.

Verfügt die beantragende Person über ein gültiges Zertifikat, kann die Beantragung weiterer Zertifikate für diese Person auch durch die Übersendung eines verschlüsselten und signierten Antrags erfolgen, sofern sich die Identität der Person nicht geändert hat.

3.2.4 Überprüfung des Domain-Namens des Antragstellers

Swisscom Digital Certificate Services überprüft den Domain-Namen des Antragstellers über eine Whois-Abfrage. Der Antragsteller muss für die Beantragung eines Zertifikats ein Bestätigungsschreiben vorlegen, das vom technischen Kontakt auf dem Whois-Auszug oder von Unterschriftsberechtigten Vertretern der Unternehmung gemäss Handelsregisterauszug unterzeichnet ist. Eine Bestätigung ist höchstens zwei Jahre gültig.

3.2.5 Nicht überprüfte Informationen

Es werden alle Informationen überprüft, die für die Identitätsprüfung erforderlich sind (Abschnitt 3.2.2 und 3.2.3). Darüber hinaus werden keine weiteren Informationen überprüft.

3.2.6 Cross-Zertifizierung

Eine Cross-Zertifizierung wird für den Service nicht angeboten.

3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung

Bei der Schlüsselerneuerung eines Zertifikates handelt es sich um die Ersetzung eines Zertifikates durch ein Zertifikat mit neuer Gültigkeitsdauer und für ein neues Schlüsselpaar, aber sonst unverändertem Inhalts. In [RFC 3647] wird dieser Vorgang „certificate re-key“ genannt.

3.3.1 Routinemässige Zertifikaterneuerung (re-key)

Eine routinemässige Zertifikaterneuerung setzt voraus, dass der Zertifikatinhaber über ein gültiges Zertifikat der zuständigen CA (Zertifikatsklasse „Smaragd“) verfügt. Dazu sollte er den Antrag auf ein neues Zertifikat vor Ablauf der Gültigkeit des zu erneuernden Zertifikates stellen. Sofern alle hinterlegten Dokumente für die Identifikation noch aktuell und gültig sind und ein gültiges Zertifikat vorliegt, sind keine zusätzlichen Massnahmen nötig. Für alle anderen Fälle ist wie für einen Neuantrag (3.2) zu verfahren.

3.3.2 Zertifikaterneuerung (re-key) nach einer Ungültigerklärung

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

3.4 Identifizierung und Authentifizierung bei einer Ungültigerklärung

Um ein Zertifikat beim CSP oder der zuständigen Registrierungsstelle als ungültig erklären zu können, wird dem Zertifikatinhaber oder der juristischen Person, für die der Zertifikatsbesitzer eine Rolle wahrnimmt, ein geeignetes Verfahren angeboten. Die Ungültigerklärung eines Zertifikats

kann telefonisch unter Angabe der mit der E-RA/TPS vereinbarten Autorisierungsinformation oder handschriftlich erfolgen. Unter bestimmten Voraussetzungen kann eine Ungültigerklärung auch elektronisch über das Webportal des CSP erfolgen, die Details sind dem CPS [8] Kapitel 3.4 zu entnehmen.

Es gelten folgende Zuständigkeiten für die Ungültigerklärung:

- Der Zertifikatsbesitzer oder die juristische Person für die der Zertifikatsbesitzer eine Rolle wahrnimmt richten einen Antrag für die Ungültigerklärung an die zuständige RA oder E-RA.
- Die RA / E-RA überprüft die Identität des Antragstellers und die Begründung für die Ungültigerklärung.
- Nach erfolgreicher Prüfung wird das entsprechende Zertifikat durch die RA / E-RA ungültig erklärt.
- Der CSP veröffentlicht die CRL mit den Ungültigerklärten Zertifikaten.

4 Betriebsanforderungen für den Zertifikats Lebenszyklus

4.1 Zertifikatantrag

4.1.1 Annahme eines Zertifikatantrages

Zertifikatanträge sind an die RA -Vertragspartner der Swisscom Digital Certificate Services zu richten. Diese können Zertifikate an den Antragsteller eines Zertifikats ausgeben, sofern die Bedingungen unter 1.3.3 erfüllt sind.

4.1.2 Registrierungsprozess

Ein Zertifikat kann durch den CSP erst erzeugt werden, wenn der Registrierungsprozess bei einer RA erfolgreich abgeschlossen wurde. Die Dokumentation des Registrierungsprozesses bei natürlichen Personen beinhaltet zumindest:

- Zertifikatantrag
- Kopie aller vorgelegter Ausweisdokumente mit einem aktuellen Lichtbild
- Bestätigung des Antragstellers eines Zertifikats, den Kundenvertrag (mit allen Bestandteilen wie Leistungsbeschreibung, Nutzungsbestimmung, AGB) gelesen und verstanden zu haben
- Aussage darüber, ob die Informationen im Zertifikat veröffentlicht werden sollen. Standardmässig werden die Daten nicht publiziert.

Für die Vertretung einer juristischen Person müssen die entsprechenden Vollmachten vorliegen, die belegen, dass der Antragsteller (natürliche Person) berechtigt ist im Namen der juristischen Person zu handeln.

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 Abschnitt 3.2 genannten Verfahren durch.

4.2.2 Annahme oder Abweisung von Zertifikatanträgen

Der Zertifizierungsantrag wird von der Registrierungsstelle oder dem CSP angenommen, wenn die folgenden Kriterien erfüllt wurden:

- Vorlage aller notwendiger Dokumente (siehe Abschnitt 4.1.2)
- Zahlung der ggf. festgelegten Gebühr (siehe Abschnitt 9.1).

Nach erfolgreicher Prüfung der oben genannten Kriterien und nach Durchführung der Identifikation und Authentifizierung wird der Zertifizierungsantrag durch den CSP weiter bearbeitet.

Sollte die Prüfung der oben genannten Kriterien oder die Identifikation und Authentifizierung eines Antragstellers eines Zertifikats nicht erfolgreich sein, wird der Zertifizierungsantrag nicht bearbeitet. Der Sachverhalt wird dokumentiert und ist dem Antragsteller unter Angabe der Gründe mitzuteilen.

4.2.3 Bearbeitungsdauer

Die Bearbeitungsdauer ist dem CPS [8] Kapitel 4.2.3 zu entnehmen.

4.3 Zertifikatausstellung

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

- durch den CSP ein fortgeschrittenes Zertifikat der Klasse „Smaragd“ ausgestellt
- das Zertifikat wird dem Antragsteller ausgehändigt, hinterlegt oder übermittelt.
- der Antragsteller über diesen Vorgang informiert (siehe 4.3.2).
- der Antragsteller über den korrekten Umgang mit dem kryptografischen Mittel instruiert
- das Dokument *Nutzungsbestimmung* mit den Rechten und Pflichten der Parteien referenziert

4.3.1 Weitere Prüfungen der Zertifizierungsstelle

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

4.3.2 Benachrichtigung des Antragstellers

Nach der Zertifikatausstellung wird dem Antragsteller eines Zertifikats in geeigneter Weise das ausgestellte Zertifikat übermittelt, publiziert oder hinterlegt.

4.4 Zertifikatakzeptanz

Der Zertifikatinhaber ist verpflichtet, die Korrektheit des eigenen Zertifikats sowie des Zertifikats des CSP nach Bearbeitung des Antrags zu verifizieren.

4.4.1 Annahme des Zertifikats

Ein Zertifikat wird durch den Zertifikatinhaber akzeptiert, wenn

- das Zertifikat verwendet wird oder
- eine explizite Äusserung erfolgt oder
- wenn innerhalb eines im CPS [8] Kapitel 4.4.1 festgelegten Zeitraums kein Widerspruch erfolgt.

Fehlerhaft ausgestellte Zertifikate hat der Antragssteller und die ausstellende RA unverzüglich beim CSP für ungültig zu erklären.

4.4.2 Veröffentlichung des Zertifikats

Es gelten die Regelungen aus Abschnitt 2.1.

4.4.3 Benachrichtigung weiterer Instanzen

Eine Benachrichtigung weiterer Instanzen ist nicht vorgesehen.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

Der Anwendungsbereich der im Rahmen dieser CP ausgestellten Zertifikate ist dem Abschnitt 1.4 zu entnehmen. Fortgeschrittene digitale Zertifikate (Zertifikatsklasse „Smaragd“) können für die Authentisierung verwendet werden.

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatinhaber

Durch Annahme des Zertifikats versichert der Zertifikatinhaber allen Teilnehmern der Swisscom Digital Certificate Services 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,
- 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,
- vor der Nutzung eines Zertifikats dessen Gültigkeit überprüfen 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 Digital Certificate Services für fortgeschrittene Zertifikate nicht unterstützt.

Bei einer Zertifikatserneuerung wird dem Zertifikatinhaber durch die zuständige RA ein neues Zertifikat basierend auf einem neuen Schlüsselpaar erzeugt, siehe Kapitel 4.7

4.6.1 Gründe für eine Zertifikaterneuerung (Certificate renewal)

Nicht anwendbar

4.6.2 Beantragung einer Zertifikaterneuerung (Certificate renewal)

Nicht anwendbar

4.6.3 Ablauf der Zertifikaterneuerung (Certificate renewal)

Nicht anwendbar

4.6.4 Benachrichtigung des Zertifikatinhabers

Nicht anwendbar

4.6.5 Annahme einer Zertifikaterneuerung

Nicht anwendbar

4.6.6 Veröffentlichung einer Zertifikaterneuerung

Nicht anwendbar

4.6.7 Benachrichtigung weiterer Instanzen über eine Zertifikaterneuerung

Nicht anwendbar

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

Bei einer Zertifikaterneuerung wird grundsätzlich ein neues Schlüsselpaar erstellt. Die Lebensdauer des Zertifikates und der Schlüssel sind gleich (3 Jahre).

Es werden die Schlüssellänge und der Algorithmus verwendet, der zu dem jeweiligen Zeitpunkt aktuell ist und gemäss Addendum zum CPS [12] Kapitel 2 einzusetzen sind. Der Zertifikatinhaber 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 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 oder direkt durch den RA-Vertragspartner beantragt, es obliegt dem CSP, ob sie eine Zertifikaterneuerung aktiv unterstützt. Entsprechende Prozesse sind dem CPS [8] Kapitel 4.6.2 zu entnehmen.

4.7.3 Ablauf Re-Key

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

4.7.4 Benachrichtigung des Zertifikatinhabers bei Re-Key

Es gelten die Regelungen gemäss Abschnitt 4.3.2.

4.7.5 Annahme eines Re-Key

Es gelten die Regelungen gemäss Abschnitt 4.4.1.

4.7.6 Veröffentlichung bei Re-Key

Es gelten die Regelungen gemäss Abschnitt 4.4.2.

4.7.7 Benachrichtigung weiterer Instanzen bei Re-Key

Es gelten die Regelungen gemäss Abschnitt 4.4.3.

4.8 Zertifikatmodifizierung

Bei der Zertifikatmodifizierung wird aufgrund von Veränderungen der Informationen im Zertifikat ein neues Zertifikat mit demselben Schlüsselpaar erstellt. Sofern sich die Identität des Zertifikatinhabers geändert hat, ist wie bei einem Neuantrag zu verfahren. Das alte Zertifikat wird nach Ausstellung des neuen Zertifikats ungültig erklärt.

Zertifikatsmodifizierungen werden nur dann durchgeführt, wenn das zugehörige Schlüsselpaar noch mindestens 12 Monate gültig ist und die Identität des Zertifikatsinhabers sich nicht ändert. Ansonsten wird eine Zertifikatserneuerung mit einem neuen Schlüsselpaar (re-key) vorgenommen.

4.8.1 Gründe für eine Zertifikatsmodifizierung

Gründe für eine Zertifikatsmodifizierung sind:

- Schreibfehler bei der Ausstellung des Zertifikates
- Modifikation einer optionalen Zertifikatsinformation (e-Mail Adresse, Organisation, etc.)

4.8.2 Beantragung einer Zertifikatsmodifizierung

Der Zertifikatsinhaber muss persönlich bei der zuständigen RA vorsprechen und einen Beleg für die zu ändernden Informationen vorlegen.

4.8.3 Ablauf einer Zertifikatsmodifizierung

Der Ablauf der Zertifikaterneuerung entspricht den Regelungen unter 4.3, für die Identifizierung und Authentifizierung bei der Zertifikatsmodifizierung gelten die Regelungen gemäss Abschnitt 3.3.1.

4.8.4 Benachrichtigung des Zertifikatinhabers bei Zertifikatsmodifizierung

Der Zertifikatsinhaber beantragt die Zertifikatsmodifizierung persönlich und muss somit nicht speziell benachrichtigt werden.

4.8.5 Annahme einer Zertifikatsmodifizierung

Es gelten die Regelungen gemäss Abschnitt 4.4.1.

4.8.6 Veröffentlichung einer Zertifikatsmodifizierung

Es gelten die Regelungen gemäss Abschnitt 4.4.2.

4.8.7 Benachrichtigung weiterer Instanzen bei einer Zertifikatsmodifizierung

Es gelten die Regelungen gemäss Abschnitt 4.4.3.

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 (ZertEs Art. 10). Einmal ungültig erklärte Zertifikate können nicht erneuert oder verlängert werden.

4.9.1 Gründe für eine Ungültigerklärung

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

1. der Zertifikatsinhaber oder die juristische Person oder Organisation, die dieser vertritt einen entsprechenden Antrag stellt, oder
2. dem CSP 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 [8] 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 dem CSP 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 [8] Kapitel 4.9 zu entnehmen. Voraussetzung für die Akzeptanz einer Ungültigerklärung des Zertifikats ist eine erfolgreiche Identifizierung und Authentifizierung des Zertifikatinhabers entsprechend Abschnitt 3.4.

4.9.3 Ablauf einer Ungültigerklärung eines Zertifikats

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

Der Inhaber des fortgeschrittenen Zertifikates wird über die Ungültigkeitserklärung umgehend informiert.

4.9.4 Fristen für den Zertifikatinhaber

Der Zertifikatinhaber muss unverzüglich die zuständige RA oder den CSP benachrichtigen und die Ungültigerklärung des eigenen Zertifikats veranlassen, wenn Gründe (siehe 4.9.1) für eine Ungültigerklärung vorliegen. Der CSP bietet auf seinem Webportal einen entsprechenden Service an, um auch ausserhalb der Geschäftszeiten der RA Anträge auf Ungültigerklärung entgegenzunehmen.

4.9.5 Fristen für die Zertifizierungsstelle

Die RA soll einen Auftrag für eine Ungültigerklärung eines Zertifikats unverzüglich bearbeiten, wenn die Voraussetzungen gegeben sind.

4.9.6 Anforderungen zur Kontrolle der CRL durch den Zertifikatprüfer

Es gelten die Regelungen gemäss Abschnitt 4.5.2.

4.9.7 Aktualisierung der CRL's

Das Aktualisierungsintervall für eine CRL ist dem CPS [8] Kapitel 4.9.7 zu entnehmen. Die CRL wird jedoch alle 2 Stunden nachgeführt.

4.9.8 Maximale Latenzzeit für CRL's

Die maximale Latenzzeit für eine CRL ist dem CPS [8] Kapitel 4.9.8 zu entnehmen.

4.9.9 Verfügbarkeit von Online-ungültigkeits-/Status-Überprüfungsverfahren

Swisscom Digital Certificate Services bietet ein Online-Verfahren an, mit dem die Gültigkeit eines Zertifikats überprüft werden kann. Es müssen dabei alle Zertifikate erfasst werden, die von der Zertifizierungsstelle ausgestellt worden sind. Details sind dem CPS [8] Kapitel 4.9.9 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

Vor jeder Nutzung eines Zertifikats sollte dessen Gültigkeit überprüft werden. Die Standards sind den Abschnitten 3 (CRL-Profil) und 4 (OCSP-Profil) des Addendums zum CPS [12] zu entnehmen.

4.9.11 Andere verfügbare Formen der Ungültigkeitsbekanntmachung

Swisscom Digital Certificate Services bietet keine anderen Verfahren zur Ungültigkeitsbekanntmachung an.

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 gesperrt.

4.9.13 Gründe für eine Suspendierung

Eine Suspendierung von fortgeschrittenen Zertifikaten der Zertifikatsklasse „Smaragd“ wird nicht unterstützt.

4.9.14 Beantragung einer Suspendierung

Nicht anwendbar.

4.9.15 Ablauf einer Suspendierung

Nicht anwendbar.

4.9.16 Begrenzung der Suspendierungsperiode

Nicht anwendbar.

4.10 Dienst zur Statusabfrage von Zertifikaten

Die Details zum Verfahren, Verfügbarkeit und dessen Merkmale sind dem CPS [8] Kapitel 4.10 zu entnehmen. Der Dienst steht grundsätzlich rund um die Uhr zur Verfügung.

4.10.1 Verfahrensmerkmale

Die Verfahrensmerkmale sind dem CPS [8] Kapitel 4.10.1 zu entnehmen.

4.10.2 Verfügbarkeit des Dienstes

Die Angaben über die Verfügbarkeit des Dienstes sind dem CPS [8] Kapitel 4.10.2 zu entnehmen.

4.10.3 Optionale Merkmale

Die optionalen Dienstmerkmale sind dem CPS [8] Kapitel 4.10.3 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). Die Aufbewahrungsdauer von Dokumenten und Zertifikaten entspricht den Vorgaben des ZertES von 11 Jahren.

4.12 Schlüsselhinterlegung und -wiederherstellung

Schlüsselhinterlegung und –Wiederherstellung (Key-Escrow and Recovery) wird für fortgeschrittene Signaturschlüssel der Stufe Smaragd seitens Swisscom Digital Certificate Services nicht angeboten.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen

Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen sind dem CPS [8] Kapitel 5 zu entnehmen. Einzelne Bereiche können in eigenständigen Dokumenten vorliegen, die nicht zwingend veröffentlicht werden. Alle Sicherheitsmassnahmen entsprechen den Vorgaben des ZertES [1], den TAV [3] sowie den anderen referenzierten Dokumenten, insbesondere dem ETSI TS 101 456 [5].

6 Technische Sicherheitsmassnahmen

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

7 Profile für Zertifikate, Widerrufslisten und Online-Statusabfragen

Von Swisscom Digital Certificate Services ausgestellte fortgeschrittene Zertifikate der Zertifikatsklasse „Smaragd“, die Widerrufsliste (CRL) und Online-Statusabfragen (OCSP) basieren auf den Vorgaben des ZertES [1], den TAV [3] sowie anderen den referenzierten Dokumenten, insbesondere dem ETSI TS 101 456 [5] und sind im Addendum zum CPS [12], detailliert beschrieben.

7.1 Zertifikatprofil

Die Details des Zertifikatsprofiles sind dem Addendum zum CPS [12], Kapitel 2zu entnehmen.

7.1.1 Zertifikaterweiterungen

Die Details der Zertifikatsprofilerweiterung sind dem Addendum zum CPS [12], Kapitel 2zu entnehmen.

7.2 CRL Profile

7.2.1 CRL Version

Die Details des CRL Profiles sind dem Addendum zum CPS [12], Kapitel 3zu entnehmen.

7.2.2 CRL Erweiterungen

Die Details zu CRL Erweiterungen sind dem Addendum zum CPS [12], Kapitel 3zu entnehmen.

7.3 OCSP Profile

Die Details des OCSP Profile sind dem Addendum zum CPS [12], Kapitel 4zu entnehmen.

8 Konformitätsprüfung (Compliance) und andere Assessments

Der CSP und die Registrierungsstellen der RA-Vertragspartner, welche fortgeschrittene Zertifikate ausstellen, sind verpflichtet, alle ihre Abläufe dieser CP und dem CPS [8] entsprechend auszugestalten.

Swisscom Digital Certificate Services erfüllt alle Vorgaben des ZertES [1] und daraus abgeleiteten technischen und administrativen Vorschriften. Die Einhaltung wird gemäss TAV[3], Kapitel 2 „System für die Anerkennung der CA“ durch die von einer durch die schweizerische Akkreditierungsstelle akkreditierte Anerkennungsstelle überprüft. Siehe dazu auch http://www.seco.admin.ch/sas/Akkreditierung.

Die Einhaltung der Vorgaben des ESTV für fortgeschrittene Zertifikate wird durch eine unabhängige interne Revision jährlich überprüft und festgehalten.

8.1 Intervall und Umstände der Überprüfung

Da sich die Smaragd CA in die Prozesse und physikalische Infrastruktur der nach ZertES zertifizierten Umgebung der Swisscom Digital Certificate Services eingebettet ist, profitiert diese von den jährlich wiederkehrenden Audits der Anerkennungsstelle. Zusätzlich ist der CSP gemäss TAV[3] 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 Registrierungsstellen der RA Vertragspartner.

8.2 Identität und Qualifikation der Überprüferin

Die jährlich wiederkehrende Konformitätsprüfung wird durch KPMG AG, Zürich, 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 (http://www.sas.ch/de/sas-index.html).

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. KPMG und die interne Revision 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 zuständige Anerkennungsstelle festgelegt. Für Risiken, die zwingend eine Überprüfung notwendig machen, können bestimmte Bereiche im Voraus festgelegt werden.

Die interne Revision erstellt in Absprache mit der Anerkennungsstelle 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 spätestens innerhalb 6 Monaten.

8.6 Veröffentlichung der Ergebnisse

Anleitungen zur Behebung oder allfällige Umgehungsmassnahmen zu gravierenden Mängel werden den betroffenen umgehend bekannt gemacht.

Eine allgemeine Veröffentlichung der Prüfungsergebnisse ist nicht vorgesehen.

9 Rahmenvorschriften

9.1 Gebühren

Die Gebühren für Dienstleistungen, die durch Swisscom Digital Certificate Services erbracht werden, sind der Preisliste zu entnehmen. Diese kann bei der in Abschnitt 1.5 angegebenen Kontaktadresse angefordert werden. Die Preisliste der RA-Vertragspartner (E-RA's/TPS's) sind direkt bei der entsprechenden E-RA/TPS anzufordern. Zusätzliche Leistungen, die nicht durch die Preisliste abgedeckt sind, können gesondert in Rechnung gestellt werden.

9.2 Finanzielle Verantwortung

9.2.1 Versicherungsschutz

Der Versicherungsschutz der Swisscom Digital Certificate Services erstreckt sich auf die gesetzlichen Haftpflichtansprüche gemäss den „Allgemeinen Geschäftsbedingungen (AGB) für Geschäftskunden".

Der Zertifikatsinhaber und die RA sind für einen ausreichenden Versicherungsschutz selbst verantwortlich.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertraulich zu behandelnde Daten

Jegliche Informationen über Teilnehmer und Antragsteller, die nicht unter 9.3.2 fallen, werden als vertrauliche Informationen eingestuft. Zu diesen Informationen zählen u.a. Geschäftspläne, Vertriebsinformationen, Informationen über Geschäftspartner und ebenso alle Informationen, die beim Registrierungsprozess zur Kenntnis gekommen sind.

9.3.2 Nicht vertraulich zu behandelnde Daten

Jegliche Informationen, die in den herausgegebenen Zertifikaten und der CRL explizit (z.B. Elemente des DN, E-Mail-Adresse) oder implizit (z.B. Daten über die Zertifizierung) enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft.

9.3.3 Verantwortlicher Umgang mit vertraulichen Daten

Als CSP trägt Swisscom (Schweiz) AG die Verantwortung für die Anwendung von Massnahmen zum Schutz vertraulicher Informationen. Daten dürfen nur im Rahmen der Diensterbringung bearbeitet und an Dritte nur weitergegeben werden, wenn zuvor eine Vertraulichkeitserklärung unterzeichnet wurde und die beteiligten Mitarbeiter zur Einhaltung der gesetzlichen Datenschutzbestimmungen verpflichtet wurden. Nicht als Dritte gelten die RA-Vertragspartner, die im Rahmen der Bearbeitung des Zertifikatsantrags Daten an den CSP weitergeben oder Daten vom CSP erhalten. Zu Prüf- und Revisionszwecken können Dokumente im Beisein des Security Officers der Swisscom Digital Certificate Services oder eines namentlich benannten Vertreters eingesehen werden.

9.4 Schutz von Personendaten (Datenschutz)

Im Umgang mit Daten hält sich Swisscom (Schweiz) AG als CSP an die geltende Gesetzgebung, insbesondere an das Fernmeldegesetz (FMG) und das Bundesgesetz über den Datenschutz (DSG). Der CSP erhebt, speichert und bearbeitet nur die Daten, die für die Erbringung der Leistungen, für die Abwicklung und Pflege der Kundenbeziehungen (d. h. für die Gewährleistung einer hohen Leistungsqualität), für die Sicherheit von Betrieb und Infrastruktur sowie für die Rechnungsstellung benötigt werden.

Die Anforderungen des Bundesgesetzes über den Datenschutz (DSG) werden gemäss Artikel 14 ZertES [1] eingehalten.

Zur Verhinderung von Missbrauch der Daten von SPAM Versendern können insbesondere Email – Informationen, sofern im Zertifikat enthalten, nur von authentisierten Benutzern abgefragt werden. Es werden keine e-Mail Adressen an nicht registrierte Benutzer geliefert. Im LDAP Verzeichnis werden keine Wildcard Abfragen unterstützt.

9.4.1 Nicht vertraulich zu behandelnde Daten

Entfällt.

9.4.2 Verantwortlicher Umgang mit Daten

Swisscom und die von ihr beauftragten Registrierungsstellen halten sich im Umgang mit Personendaten an das Datenschutz (DSG)- und Fernmelderecht (FMG).

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

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 DSG).

Mit Personendaten darf kein Handel betrieben werden (Art. 14 Abs. 1 ZertES).

9.4.3 Nutzung von Personendaten

Es gelten die Regelungen gemäss Kapitel 9.4.2.

9.4.4 Offenlegung bei gerichtlicher Anordnung oder im Rahmen einer gerichtlichen Beweisführung

Swisscom Digital Certificate Services als CSP unterliegt schweizerischem Recht und muss ihre Kundendaten bei Vorliegen entsprechender Entscheidungen an staatliche Organe in Übereinstimmung mit den geltenden Gesetzen freigeben.

9.4.5 Andere Umstände einer Weitergabe an Dritte

Es sind keine weiteren Umstände für eine Weitergabe an Dritte vorgesehen.

9.5 Immaterialgüterrechte

Swisscom ist Eigentümerin der Immaterialgüterrechte an folgenden Dokumenten:

- Vorliegende CP
- Dazugehöriges CPS [8]
- Markenrechte, insbesondere an Swisscom Digital Certificate Services, sowie an den weitern Vertragsdokumenten.

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

9.6 Zusicherung und Gewährleistung

9.6.1 Verpflichtung der Zertifizierungsstelle

Swisscom (Schweiz) AG verpflichtet sich als CSP alle im Rahmen dieser CP und dem CPS [8] beschriebenen Aufgaben gemäss den Vorgaben des ZertES [1] und der Ausführungsbestimmungen (TAV [3]) durchzuführen.

9.6.2 Verpflichtung der RA-Vertragspartner und Registrierungsstellen

Die RA-Vertragspartner werden vertraglich verpflichtet, alle Anforderungen gemäss Signaturgesetz sowie TAV [3] Kapitel „3.4.1 Registrierung, Verwaltung und Ungültigerklärung von Zertifikaten für Dritte“ einzuhalten.

Jeder im Namen von Swisscom operierende RA-Vertragspartner wird von Swisscom verpflichtet, alle in dieser CP und in der zugehörigen CPS [8] beschriebenen Aufgaben durchzuführen. Die Einhaltung der jeweiligen CP muss durch den RA Betreiber gegenüber dem CSP schriftlich zugesichert werden. Ebenso sind die Rollen und Zuständigkeiten der RA durch den CSP zu dokumentieren und zu kommunizieren.

9.6.3 Verpflichtung des Zertifikatinhabers

Es gelten die Regelungen von Kapitel 4.5.1.

9.6.4 Verpflichtung des Zertifikatprüfers

Es gelten die Regelungen von Kapitel 4.5.2.

9.6.5 Verpflichtung anderer Teilnehmer

Sofern weitere Teilnehmer als Dienstleister in den Zertifizierungsprozess eingebunden werden, ist Swisscom (Schweiz) AG als beauftragender CSP in der Verantwortung, den Dienstleister zur Einhaltung der CP und CPS [8] zu verpflichten.

9.7 Ausschluss der Gewährleistung

Entfällt

9.8 Haftung von Swisscom (Schweiz) AG

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

Swisscom (Schweiz) AG haftet nicht für Schäden, die sich aus der Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung im Zertifikat ergeben (gemäss Art. 7. Abs 2 und Art. 16 Abs. 3 ZertES [1]).

In allen anderen Fällen haftet Swisscom (Schweiz) AG 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 zum Betrage von CHF 500'000 je Schadenereignis und für Vermögensschäden höchstens bis zum Betrag von CHF 50'000 je Schadenereignis.
- In keinem Fall haftet Swisscom für Folgeschäden, insbesondere entgangenen Gewinn oder Daten- oder Reputationsverluste.

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

9.9 Haftung des Zertifikatinhabers

Für die Verwendung gemäss Kapitel 1.4 des dem Zertifikat zu Grunde liegenden geheimen Schlüssels haftet ausschliesslich der Zertifikatinhaber.

Der Zertifikatinhaber haftet gemäss der vertraglichen Vereinbarung mit der RA für Schäden, die diese erleidet, weil er seinen vertraglichen Verpflichtungen (insbesondere den Vereinbarungen für die Nutzung des Zertifikats) nicht nachgekommen ist. Swisscom (Schweiz) AG kann gegenüber dem Zertifikatsinhaber bei Verletzung des RA-Vertragsverhältnisses ausservertragliche Haftungsansprüche geltend machen.

Für Organisationszertifikate ist gegenüber Dritten in keinem Fall der Antragsteller, sondern die Organisation, welche im O-Feld des Zertifikates genannt ist, durch die Verwendung des Zertifikats gebunden und somit für alle Handlungen die mit dem Zertifikat oder im Zusammenhang mit der Nutzung des Zertifikates begangen werden, verantwortlich. Der Antragsteller ist aber für den Erlass schriftlicher organisationsinterner Weisungen verantwortlich, die den Einsatz des Zertifikats, den Zugang zum Zertifikat und dessen allfällige Sperrung festhalten (z.B. Aufbewahrung der Smartcard, des Passwortes, des Sperrkennwortes, usw.).

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Diese CP und das zugehörige CPS [8] treten an dem Tag in Kraft, an dem sie über den Informationsdienst (siehe Abschnitt 2.2) der Swisscom Digital Certificate Services veröffentlicht werden.

9.10.2 Aufhebung

Dieses Dokument ist gültig, bis

- es durch eine neue Version ersetzt wird oder
- der Betrieb der der Swisscom Digital Certificate Services als CSP eingestellt wird.

9.10.3 Konsequenzen der Aufhebung

Von einer Aufhebung der CP und dem CPS [8] bleibt die Verantwortung zum Schutz vertraulicher Informationen und personenbezogener Daten sowie allenfalls weiter darüber hinaus bestehender Pflichten der Parteien unberührt.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

Der CSP informiert die Zertifikatinhaber bei Kenntnis der E-Mail Adresse via signierte E-Mail oder via Brief.

Die Kommunikation mit den übrigen Teilnehmern erfolgt mittels signierten Formularen via E-Mail oder Brief. Ankündigungen und News werden auf der Homepage von Swisscom (Schweiz) AG publiziert.

9.12 Änderungen der Richtlinien

Es besteht ein formelles Genehmigungsverfahren für die CP und Änderungen davon.

9.13 Konfliktbeilegung

Alle sich aus der vorliegenden CP ergebenden Streitigkeiten, an denen Swisscom (beteiligt ist, sind nach den Bestimmungen des Konkordates über die Schiedsgerichtsbarkeit einem Dreierschiedsgericht mit Sitz in Bern zur endgültigen Entscheidung zu unterbreiten. Die Bestellung des Schiedsgerichts erfolgt durch den Präsidenten des Handelsgerichts des Kantons Bern. Das Verfahren vor dem Schiedsgericht richtet sich nach der Zivilprozessordnung des Kantons Bern, soweit nicht das Konkordat über die Schiedsgerichtsbarkeit zur Anwendung gelangt. Die Verhandlung wird in deutscher Sprache geführt.

Die Vertragspartner verpflichten sich jedoch, vor Anrufung des Schiedsgerichts alle zumutbaren Anstrengungen zu unternehmen, den Streit einvernehmlich beizulegen. Sie können sich dazu eines gemeinsam zu bestimmenden Mediators bedienen.

Ein solcher Vermittlungsversuch hat keine Auswirkung auf gesetzliche Verjährungsfristen.

9.14 Geltendes Recht und Gerichtsstand

Anwendbares Recht für die Swisscom Digital Certificate Services CP ist die schweizerische Gesetzgebung, insbesondere das schweizerische Signaturgesetz ZertES [1]. Ausschliesslicher Gerichtsstand ist Bern, Schweiz.

9.15 Konformität mit dem geltenden Recht

Swisscom (Schweiz) AG erhebt den Anspruch, ein CSP im Sinne des schweizerischen Signaturgesetzes [ZertES] zu sein und fortgeschrittene Zertifikate auszustellen. Es werden Zertifikate ausgestellt, mit denen fortgeschrittenen elektronische Signaturen, Verschlüsselungen und Authentisierungen gemäss dem schweizerischen Signaturgesetz erzeugt werden können. Fortgeschrittene Zertifikate sind gemäss OR Art. 14 Abs. 2bis von Gesetzes wegen der eigenhändigen Unterschrift jedoch nicht gleichgestellt.

9.16 Weitere Bestimmungen

9.16.1 Geltungsbereich

Alle in CP und CPS [8] enthaltenen Regelungen gelten zwischen Swisscom Digital Certificate Services als CSP und den RA's. Die RA's verpflichten sich diese Regelungen ihrerseits entsprechend in die Verträge zwischen ihnen und den Zertifikatinhabern zu integrieren. Falls Swisscom Digital Certificate Services mit den Zertifikatsinhabern direkt Verträge abschliesst, werden sie in diese integriert.

9.16.2 Sprache

Um die internationale Zusammenarbeit mit anderen Zertifizierungsstellen zu ermöglichen, werden Übersetzungen des CPS veröffentlicht. Im Zweifelsfalle ist die deutsche Version des Textes rechtlich verbindlich.

9.16.3 Gültigkeit

Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen.

9.16.4 Änderungen der CP

Es besteht ein formelles Genehmigungsverfahren für die CP und Änderungen davon.

9.16.5 Übertragung der Rechte und Pflichten

Der Zertifikatinhaber kann seine Rechte und Pflichten nicht übertragen. Swisscom kann ihre Rechte und Pflichten auf Dritte übertragen, insbesondere auf andere Swisscom Gruppengesellschaften.

10 Appendix: Translation from elected section in English

10.1 „1.1 Overview”

Swisscom Digital Certificate Services conforms to the current version of the baseline requirements for the issuance and management of publicly-trusted certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document.

10.2 „3.2 Identity verification for new application”

10.2.1 “3.2.2 Authentication of a legal entity”

Legal entities are identified through an official representative. I.e. persons applying for an emerald certificate for an organization or legal entity shall present a proof in the form of a valid power of attorney or a certification of a RA that they act on behalf of the legal entity or organization. Furthermore the statements in section 3.2.3 shall be applied.

10.2.2 “3.2.3 Authentication of a natural person”

Identity verification of a natural person or of a legal person, for which the applicant performs a role, to apply for advanced certificates are performed following these steps:

1. The applicant of a certificate sends one or more documents to the RA confirming his identity.
2. An RA employee performs the identity check based on the document provided by the applicant and documents this process.
3. For all attributes to be placed into the certificate are verified.

In case the applicant has a valid certificate, additional certificates for that person can be requested by sending a signed and encrypted application unless the identification of the person is still valid.

10.2.3 “3.2.4 Checking the domain name of the applicant”

Swisscom Digital Certificate Services checks the domain name of the applicant based on a Whois query. Applicants applying for a certificate have to submit a letter of confirmation that is signed by the technical contact stated in the Whois extract or by representatives of the company authorized to sign according to the certificate of registration. A letter of confirmation is valid for two years at most.