Swisscom
Digital Certificate Services
Zertifizierungspolitik (CP)

- Zertifikatsklasse: „Quartz“ (Extended-Validation-Zertifikat) -

Abstract	Zertifizierungspolitik für Extended-Validation-Zertifikate der Swisscom Digital Certificate Services, einer Dienstleistung der Swisscom (Schweiz) AGzur Vergabe von digitalen Zertifikaten für die SSL-/TLS-Authentifizierung und -Verschlüsselung gemäss den Richtlinien für die Ausstellung und Verwaltung von Extended-Validation-Zertifikaten („Guidelines for the Issuance and Management of Extended Validation Certificates“).
Name	**008_cp_quartz_ev_sdcs_2.16.756.1.83.4_v2.2_de(pdf).doc**
Version	**2.2**
Klassifizierung	Nicht klassifiziert
Projektname	„Hermes“
OID	**2.16.756.1.83.8 (Quartz CA 2)** **2.16.756.1.83.21.2.1 (Quartz CA 1)**
Zugehörige CPS	**CPS Swisscom Digital Certificate Services 2.16.756.1.83.2.1** **Swisscom Root EV CA 1 (OID: 2.16.756.1.83.8:2.16.756.1.83.8)** **Swisscom Root EV CA 2 (OID: 2.16.756.1.83.20.1.1: 2.16.756.1.83.20.1.1))**
Name der CA	Swisscom Quartz EV CA 1 Swisscom Quartz EV CA 2
Inhaber der CA	**Swisscom (Schweiz) AG**
Sprachfassung:	Deutsch (Rechtlich verbindliche Originalversion)
Beginn der CP-Konformitätsprüfung	1. März 2008 (Swisscom Quartz EV CA 1) 1. Januar 2011 (Swisscom Quartz EV CA 2)
Genehmigung des Dokuments	Swisscom (Schweiz) AG, Governance Board
Unterschrift	_____

Änderungskontrolle

Version	Datum	Geändert von	Bemerkungen/Art der Änderung
1.0	26.02.08	Patrick Graber	Ergänzungen KPMG
1.1	03.04.09	Udo Rothmann	Aktualisierung
1.2	29.09.09	Udo Rothmann	Kleine Anpassungen
1.3	06.11.09	Udo Rothmann	Kleine Anpassungen
1.4	23.11.2009	Willfried Braun	Kapitel 4 von CPS (Addendum) in CP überführt
2.0	11.11.2011	Projektteam	Ergänzt mit SHA-256 CA Hierarchie.
2.1	01.02.2012	Projekt Team	Typos korrigiert
2.2	1.4.2012	Projekt Team	Update CAB Referenz

Freigabe

Version	Datum	Freigabestelle	Bemerkungen/Art der Änderung
1.4	13.04.2011	Governance Board	
2.0	21.11.2011	Governance Board	

Referenzierte Dokumente

Referenz	Bezeichnung
[1]	**ZertES**: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES) vom 19. Dezember 2003, nachfolgend „Schweizerisches Signaturgesetz“ genannt.
[2]	**VZertES**: Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (Verordnung über die elektronische Signatur, VZertES) vom 3. Dezember 2004
[3]	**TAV**: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur, Ausgabe 4: 01.08.2011, SR 943.032.1/Anhang
[4]	**IETF RFC 3647** (2003): „Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework“
[5]	**ETSI TS 101 456 V1.4.1** (2007-05): Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates
[6]	**IETF RFC 5280** (May 2008) „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“ **(**Obsoletes: RFC 3280, RFC 4325, RFC 4630**)**
[7]	**IETF RFC 2560** (1999) „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]	**Richtlinien des CA/Browser-Forums** für die Ausstellung und Verwaltung von Extended-Validation-Zertifikaten („Guidelines for the Issuance and Management of Extended Validation Certificates“), Version 1.3 [http://cabforum.org/Guidelines_v1_3.pdf]
[10]	**IETF RFC1034 (November 1987)** - DOMAIN NAMES - CONCEPTS AND FACILITIES
[11]	**IETF RFC2460 (December 1998)** - Internet Protocol, Version 6 (IPv6) pecification)

swisscom

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument beschreibt die Zertifizierungspolitik (Certificate Policy, nachfolgend „CP“ genannt) von Swisscom Digital Certificate Services, einer Dienstleistung der Swisscom (Schweiz) AG (nachfolgend „Swisscom“ genannt), zur Vergabe von fortgeschrittenen, digitalen Extended-Validation-Zertifikaten.
Die CP erlaubt Zertifikatsprüfern die Vertrauenswürdigkeit jener Zertifikate zu beurteilen, die von Swisscom als Anbieterin von Zertifizierungsdiensten (Certification Service Provider, nachfolgend „CSP“ genannt) und ihren RA-Vertragspartnern ausgestellt werden.
Ein „Quartz“ Zertifikat ist eine elektronische Bescheinigung, mit der einer Person oder Organisation ein öffentlicher kryptografischer Schlüssel zugeordnet wird, um ihre Identität zu bestätigen. Ein Zertifikat stellt somit eine Verbindung zwischen einer Person oder Organisation und einem kryptografischen Schlüssel her.
In Bezug auf elektronische Signaturen wird die Bezeichnung „Extended Validation“ (nachfolgend „EV“ genannt) gemäss CA/Browser-Forum folgendermassen definiert:

- **Wichtigste Zwecke:** EV-Zertifikate dienen in erster Linie
  1. der Identifikation der juristischen Person, die eine Website betreibt. Dem Benutzer eines Internetbrowsers wird so versichert, dass die vom Benutzer aufgerufene Website von einer juristischen Person betrieben wird, deren Daten (Name, Sitz, Gerichtsstand und Handelsregisternummer) im EV-Zertifikat hinterlegt sind;
  2. der aktivierten und verschlüsselten Kommunikation mit einer Website. Der Austausch von Schlüsseln wird vereinfacht, damit die verschlüsselte Datenkommunikation zwischen dem Benutzer des Internetbrowsers und der Website via Internet ermöglicht wird.
- **Zusätzliche Zwecke:** Mithilfe von EV-Zertifikaten wird die Legitimität des Unternehmens, das als Betreiber einer Website angegeben wird, durch eine Bestätigung der rechtlichen und physischen Existenz des Unternehmens nachgewiesen. EV-Zertifikate können auch bei Problemen nützlich sein, die in Verbindung mit Phishing und anderen Formen des Online-Identitätsdiebstahls auftreten. Durch die Bereitstellung von zuverlässigeren, durch Dritte verifizierten Informationen zur Identität und Adresse eines Website-Betreibers können EV-Zertifikate in folgenden Bereichen hilfreich sein:
  3. Erschweren von Phishing- oder sonstigen Angriffen im Zusammenhang mit Online-Identitätsdiebstahl unter Verwendung von SSL-Zertifikaten;
  4. Unterstützung von Unternehmen, auf die Phishing- oder sonstige Angriffe im Zusammenhang mit Online-Identitätsdiebstahl verübt werden könnten, indem ihnen ein Instrument zur Verfügung gestellt wird, mit dem sie ihre Identität und ihre legitimierte Website gegenüber Benutzern besser ausweisen können;
  5. Unterstützung der Strafverfolgung bei Ermittlungen zu Phishing- und sonstigen Angriffen im Zusammenhang mit Online-Identitätsdiebstahl, ggf. einschliesslich Kontaktaufnahme, Untersuchungen oder Einleiten rechtlicher Schritte gegen die betreffende Person.

- **Nicht abgedeckte Zwecke:** EV-Zertifikate erlauben nur Rückschlüsse auf die Identität der im Zertifikat angegebenen Person, nicht auf deren Verhalten. Daher gewähren EV-Zertifikate ***keine*** Sicherheiten bzw. bezeugen oder gewährleisten ***nicht***, dass
  6. die im EV-Zertifikat angegebene Person aktiv Geschäfte betreibt;
  7. die im EV-Zertifikat angegebene Person sich an die geltende Gesetzgebung hält;
  8. die im EV-Zertifikat angegebene Person im Hinblick auf ihre Geschäftstätigkeit vertrauenswürdig, rechtschaffen oder seriös ist;
  9. das Betreiben von Geschäften mit der im EV-Zertifikat angegebenen Person „sicher“ ist.

Jedes Zertifikat ist nur so vertrauenswürdig wie die Verfahren, nach denen es ausgestellt wird. Für die Zertifikatsklasse „Quartz“ muss sich der zu Zertifizierende persönlich an eine RA wenden und alle im Zertifikat angegebenen Daten mit amtlichen Ausweisen oder Bescheinigungen belegen. Die

detaillierten Verifizierungsprozesse, auf denen die Zertifikatsklasse basiert, sowie die allgemeinen angewandten Sicherheitsvorkehrungen können dem Certification Practice Statement (nachfolgend „CPS“ genannt) der Swisscom Digital Certificate Services entnommen werden.
Diese CP bezieht sich auf die Zertifikatsklasse „Quartz“ und entspricht den Anforderungen des CA/Browser-Forums für die Ausstellung und Verwaltung von Extended-Validation-Zertifikaten (Guidelines for the Issuance and Management of Extended Validation Certificates [9]). Für alle Zertifikate, die dieser CP entsprechen, ist der Object Identifier gemäss X.509 [OID] im Zertifikat angegeben. Somit wird die CP an das Zertifikat einer bestimmten Zertifikatsklasse gebunden.
Die Zertifikatsklasse „Quartz“ erfordert keine sichere Signaturerstellungseinheit (nachfolgend „SSCD“ genannt). Das fortgeschrittene Zertifikat eignet sich für den Nachweis der Identität (Authentizität) einer Organisation und für den sicheren Austausch von Schlüsseln. Diese Zertifikatsklasse wird an Organisationen vergeben und kann zur Unterzeichnung von Transaktionen jeder Art, insbesondere jedoch für TLS-Übertragungen in SSL-Sitzungen, verwendet werden.
Swisscom garantiert, dass „Quartz“ Zertifikate in derselben Infrastruktur und mit denselben Prozessen betrieben werden wie die Zertifikatsklasse „Diamant“ und damit die Vorgaben des Signaturgesetzes (ZertES [1]), der Verordnung über die elektronische Signatur (VzertES [2]), der technischen und administrativen Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur vom 13.11.2006 (TAV [3]) und des aufgeführten ETSI TS 101 456 erfüllt. Die Einhaltung dieser Vorgaben wird von einer von der Schweizerischen Akkreditierungsstelle (SAS) akkreditierten Anerkennungsstelle geprüft.
Die vorliegende 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 CP wurde von Swisscom zu folgendem Zweck erstellt:

- Erfüllung der Anforderungen an CSP, die EV-Zertifikate ausstellen, gemäss den Vorgaben des CA/Browser-Forums [9];
- Beschreibung der Dienstleistungen, Rollen, Einschränkungen und Verpflichtungen im Zusammenhang mit der Verwendung von Zertifikaten der Zertifikatsklasse „Quartz“ der Swisscom Digital Certificate Services;
- Sicherstellung der Interoperabilität bei der Benutzung fortgeschrittener Zertifikate der Swisscom Digital Certificate Services.

Die CP basiert auf den Vorgaben des RFC 3647 [4]. Die Rahmen für CP und CPS wurden nach den für Dienstanbieter von qualifizierten und fortgeschrittenen Zertifikaten geltenden Vorgaben und gemäss den folgenden Vorschriften festgelegt:

- SR 943.023.1 [3]
- ETSI TS 101 456 [5]
- CA/Browser-Forum [9].

Um die internationale Zusammenarbeit mit anderen CA zu vereinfachen, wird die CP auch in englischer Übersetzung veröffentlicht; massgeblich ist jedoch in jedem Fall die deutsche Version in der jeweils aktuellen Fassung.

1.2 Identifikation des Dokuments

Identifikation Swisscom Quartz EV CA 1

- Titel: Swisscom Digital Certificate Services – Zertifizierungspolitik (CP)
- Version: 1
- Object Identifier (OID): 2.16.756.1.83.8
- Zusammensetzung der OID:

1. Stelle	2. Stelle	3. Stelle	4. Stelle	5. Stelle	6. Stelle	7. Stelle	**Bedeutung**
2							Joint ISO-CCITT Tree
	16						Land
		756					Schweiz
			1				Organisationsname (RDN)
				83			Swisscom Digital Certificate Services [1]
					8		Klasse: fortgeschritten (Quartz CA 1)
						1	Zertifizierungspolitik (CP)

Identifikation Swisscom Quartz EV CA 2

- Titel: Swisscom Digital Certificate Services – Zertifizierungspolitik (CP)
- Version: 2.0
- Object Identifier (OID): 2.16.756.1.83.21.2.1
- Zusammensetzung der OID:

1. Stelle	2. Stelle	3. Stelle	4. Stelle	5. Stelle	6. Stelle	7. Stelle	6. Stelle	**Bedeutung**
2								Joint ISO-CCITT Tree
	16							Land
		756						Schweiz
			1					Organisationsname (RDN)
				83				Swisscom Digital Certificate Services [2]
					21			Klasse: fortgeschritten (Quartz CA 2)
						2		Zertifizierungspolitik (CP)
							1	Version

Die vom BAKOM für die verschiedenen Kategorien vergebenen OID können auf der Website der BAKOM unter „RDN“ (Relative Distinguished Name, Name eines Verzeichniseintrags) eingesehen werden (http://www.e-ofcom.ch).

[1] Durch Bundesamt für Kommunikation (BAKOM) zugeteilt.

[2] Durch Bundesamt für Kommunikation (BAKOM) zugeteilt.

1.3 Beteiligte der Swisscom Digital Certificate Services

1.3.1 Zertifizierungsstellen (CA)

Als akkreditierte Anbieterin von Zertifizierungsdiensten betreibt Swisscom eine Offline Root Certification Authority (nachfolgend „CA" genannt) sowie eine der Root-CA untergeordnete CA für EV-SSL-Zertifikate („Quartz").

Die Swisscom-Root-CA ist an kein Netzwerk angeschlossen und wird nur bei Bedarf gestartet. Die Root-CA stellt ausschliesslich Zertifikate für unmittelbar nachgelagerte CA der Swisscom Digital Certificate Services aus. Die Quartz-CA vergibt Zertifikate an juristische Personen und Organisationen.

- Diese CP bezieht sich nur auf die Zertifikatklasse, dem fortgeschrittenen digitalem Zertifikat „Quartz" und entspricht den Anforderungen des CA/Browser-Forum [9].

Die Infrastruktur ist folgendermassen aufgebaut [8]

1.3.2 Registrierungsstellen (RA)

Das Geschäftsmodell von Swisscom basiert auf einem Modell mit Vertragspartnern als Registrierungsstellen (Registration Authorities, nachfolgend „RA" genannt). Dabei übernehmen Vertragspartner von Swisscom die Funktion der RA.

Das Geschäftsmodell von Swisscom unterscheidet zwei Typen von RA (Swisscom/Partner):

- **Swisscom-RA**: vergeben Zertifikate für den Firmengebrauch, für Kunden und die nachgelagerten RA (E-RA);
- **Enterprise-RA** (Enterprise Registration Authority nachfolgend „E-RA" genannt): ein RA-Partner, der Zertifikate direkt erstellen und vergeben kann;
- **TPS** (Trusted Point of Sale): ein RA-Partner, der als RA Zertifikatsanträge entgegennimmt und die Angaben überprüft.

Bei einer RA, die „Quartz"-Zertifikate vergeben, werden regelmässig überprüft, um die Einhaltung der Geschäftsbedingungen von Swisscom und des CA/Browser-Forums sicherzustellen.

Die RA-Vertragspartner werden vertraglich verpflichtet, alle Anforderungen gemäss CA/Browser-Forum [9] Kapitel *„10 Information Verification Requirements"* einzuhalten.

Eine E-RA stellt sicher, dass der Antragsteller umfassend über die für die Verwendung eines Zertifikats geltenden Geschäftsbedingungen und die damit verbundenen Verbindlichkeiten aufgeklärt wurde und er diese verstanden hat. Die Rollen und Zuständigkeiten der E-RA sind durch den CSP zu dokumentieren und zu kommunizieren.

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.

1.3.3 Zertifikatsinhaber

Quartz-EV-SSL/TLS-Zertifikate werden an private Organisationen, staatliche Stellen oder Wirtschaftsunternehmen vergeben. In jedem Fall muss eine natürliche Person bei der RA persönlich vorstellig werden, sich unter Vorlage eines amtlichen Ausweises als Zertifikatsinhaber registrieren und sich dazu verpflichten, die Nutzungsbestimmungen einzuhalten oder für deren Einhaltung Sorge zu tragen. Nur durch die RA registrierte Personen können Änderungen, Aktualisierungen und eine Ungültigerklärung des Zertifikats veranlassen. Wenn ein registrierter Zertifikatsinhaber während der Gültigkeitsdauer des Zertifikats eine juristische Person verlässt oder eine juristische Person einer natürlichen Person die Vollmacht zur Vertretung der juristischen Person entzieht, muss sich ein Nachfolger bei der RA registrieren. Während der Gültigkeitsdauer des Zertifikats muss ständig eine natürliche Person bei der RA als Bevollmächtigter registriert sein.

1.3.4 Zertifikatsprüfer

Zertifikatsprüfer sind natürliche Personen oder Organisationen, die unter Nutzung eines von Swisscom Digital Certificate Services ausgestellten Zertifikats die Identität des Webservers eines Zertifikatsinhabers überprüfen, um so einen sicheren und zuverlässigen elektronischen Datenaustausch zu ermöglichen. Ein Zertifikatsprüfer kann – muss aber nicht – Teilnehmer von Swisscom Digital Certificate Services sein.

1.3.5 Weitere Teilnehmer

Weitere Teilnehmer können natürliche oder juristische Personen sein, die als Dienstleister am Zertifizierungs- oder Registrierungsprozess beteiligt sind. Die Verantwortung für Dienstleister, die im Namen eines Zertifikatsinhabers oder -prüfers tätig werden, liegt bei dem beauftragenden Zertifikatsinhaber.
Der Abschluss von Dienstleistungsabkommen mit einem Dienstleister sowie die Annahme von Leistungen eines Dienstleisters, der im eigenen Namen handelt, kann ausschliesslich durch die Serviceleitung der Swisscom Digital Certificate Services vorgenommen werden.

1.4 Anwendbarkeit der Zertifikate

1.4.1 Geeignete Zertifikatsnutzung

Die im Rahmen dieser CP ausgestellten Zertifikate können von Zertifikatsinhabern für die elektronische Signatur und Authentisierung - als SSL/TLS-Webserver-Zertifikate zur Sicherung der Verbindung zwischen Client (Webbrowser, webbasierte Anwendung usw.) und Webserver (Webserver, Webdienste usw.) verwendet werden. Mit Quartz-EV-Zertifikaten können Zertifikatsprüfer die Identität des Webservers eines Zertifikatsinhabers überprüfen.
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.
Für die Installation des Zertifikats auf dem eigenen Webserver gemäss den Vorgaben dieser CP ist der Zertifikatsinhaber verantwortlich.

1.4.2 Untersagte Zertifikatsnutzung

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

1.5 Verwaltung der Richtlinien

Das Dokumenten-Framework wird herausgegeben von:

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.

Abkürzungen

Begriff	*Erklärung*
CA	Certification Authority – Zertifizierungsstelle
CN	Common Name, als Teil des DN
CP	Certificate Policy – Zertifizierungspolitik
CPS	Certification Practice Statement – Aussage über die Zertifizierungspraxen
CRL	Certificate Revocation List – Liste der für ungültig erklärten Zertifikate
CSP	Certification Service Provider – Anbieterin von Zertifizierungsdiensten
DN	Distinguished Name – eindeutiger Name gemäss RFC 3739
EE	End Entity

Begriff	*Erklärung*
OCSP	Online Certificate Status Protocol
RA	Registration Authority – Registrierungsstelle
SSCD	Secure Signature Creation Device – sichere Signaturerstellungseinheit (gemäss ETSI TS 101 456)
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur vom 3. Dezember 2004
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur vom 19. Dezember 2003 (siehe [1])

2 Veröffentlichungen und Verantwortungen für den Verzeichnisdienst

2.1 Verzeichnisdienst

Als CSP stellt Swisscom Digital Certificate Services sicher, dass Informationen, die zur Validierung des von ihr verwalteten Zertifikatsstatus erforderlich sind, kostenlos über eine Internetseite und eine LDAP-Abfrage bereitgestellt werden. Zusätzliche Statusdienste sind Abschnitt 2.1 der CPS [8] zu entnehmen.
Ungültige Zertifikate werden in der Liste der für ungültig erklärten Zertifikate [nachfolgend „CRL" genannt] erfasst. Die CRL wird mindestens alle 4 (vier) Stunden aktualisiert.
Details sind Abschnitt 2.2 der CPS [8] zu entnehmen.

2.2 Veröffentlichung von Informationen zu den Zertifikaten

Als CSP veröffentlicht Swisscom Digital Certificate Services folgende Informationen:

- das Wurzelzertifikat der Swisscom Digital Certificate Services und dessen Fingerabdruck;
- Zertifikate der nächsten CA-Stufe (Level 1) und deren Fingerabdrücke
- diese CP und die zugehörige CPS [8].

Darüber hinaus werden den Zertifikatsinhabern Informationen über Swisscom Digital Certificate Services, über die korrekte Anwendung von Kryptografie und die Verwendung von Zertifikaten zur Verfügung gestellt. Adressen, über die diese Informationen und weitere Dienste bezogen werden können, sind Abschnitt 2.2 der CPS [8] zu entnehmen.

2.3 Aktualisierung der Informationen

Swisscom Digital Certificate Services aktualisiert in regelmässigen Abständen die Informationen zur Überprüfung der Gültigkeit von Zertifikaten. Der Abstand zwischen zwei Aktualisierungen beträgt höchstens 24 Stunden. Einzelheiten sind Abschnitt 2.3 der CPS [8] 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] unter 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 entsprechend der Normenserie X.500 einen eindeutigen Namen (Distinguished Name, nachfolgend „DN“ genannt). 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 in Abschnitt 3.1.1 der CPS [8] festgelegt.

3.1.2 Aussagekraft der Namen

Der DN muss den Zertifikatsinhaber eindeutig identifizieren und in einer für Menschen verständlichen Form vorliegen. Bei der Namensvergabe gelten grundsätzlich folgende Grundregeln:

- Zertifikate dürfen nur auf einen zulässig Datenverarbeitungssystem Bezeichnung des Zertifikatsinhabers 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, IP-Adressen verwendet werden. Es dürfen keine innerhalb der Swisscom Digital Certificate Services benutzte 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 Zertifikatsinhaber ermöglicht. Einzelheiten sind Abschnitt 3.1.2 der CPS [8] zu entnehmen.
Der „Distinguished Names" [6] für Datenverarbeitungssystem sind ausschliesslich Internet-Domainname, öffentliche FQDN gemäss RFC zugelassene Verfahren. Der „GeneralName" [6] für Datenverarbeitungssystem sind ausschliesslich Internet-Domainname, öffentliche FQDN gemäss RFC dNSName [RFC1034][10] bzw. öffentliche iPAddress [RFC2460] [11] zugelassene Verfahren.

3.1.3 Anonymität und Pseudonymität

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] unter 3.1.3.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Der zu verwendende Zeichensatz und die Substitutionsregelungen für Sonderzeichen sind Abschnitt 3.1.4 der CPS [8] zu entnehmen.

3.1.5 Eindeutigkeit der Namen

Vor der Zertifikatsvergabe muss die Korrektheit der Angaben zum DN durch die RA anhand gültiger amtlicher Ausweise überprüft und sichergestellt werden. Der DN eines Zertifikatsinhabers muss eindeutig sein und darf nicht an unterschiedliche Zertifikatsinhaber vergeben werden. Nur wenn ein Zertifikatinhaber mehrere Zertifikate 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. Die CA ist nicht verpflichtet, solche Rechte zu überprüfen. Allein der Zertifikatsinhaber ist für solche Überprüfungen verantwortlich. Falls die CA über eine Verletzung solcher Rechte informiert wird, wird das Zertifikat für ungültig erklärt.

3.2 Identitätsüberprüfung bei Neuantrag

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 im Trust Center des CSP signiert. Die Sicherung des privaten Schlüssels obliegt dem Zertifikats Inhabers. Die entsprechenden Verfahren werden im CPS **[8]** unter 3.2.1 beschrieben.

3.2.2 Authentifizierung einer juristischen Person

Der Zertifikatsantrag einer juristischen Person muss von einer natürlichen Person eingereicht werden, die sich gemäss 3.2.2 gegenüber der RA ausweisen muss.
Die Berechtigung zur Beantragung eines Zertifikats im Namen einer im Handelsregister eingetragenen Organisation wird durch einen beglaubigten Handelsregisterauszug bestätigt. Der beglaubigte Handelsregisterauszug darf nicht älter als ein Jahr sein und der Antragsteller muss darin als Vertretungsberechtigter der Organisation genannt sein oder über eine von einem Vertretungsberechtigten der Organisation unterzeichnete Vollmacht verfügen. Dies gilt auch, wenn das im Handelsregisterauszug genannte Unternehmen nur gemeinschaftlich vertreten werden kann.

3.2.3 Wirtschaftssubjekte mit Handelsregistereintrag

English Translation see 10.1 (3.2.3 Economic Subject with excerpt from the commercial register)

Bei Unternehmen, die im Handelsregister eingetragen sind, erfolgt die Überprüfung anhand eines Handelsregisterauszugs, aus dem hervorgeht, dass die Organisation tatsächlich existiert und welche Personen für die Organisation zeichnungsberechtigt sind. Das vorgelegte Dokument muss beglaubigt und darf nicht älter als ein Jahr sein.
Für den Erhalt eines EV-Zertifikats muss ein Unternehmen in einem der folgenden Länder im Handelsregister eingetragen sein:

- Schweiz

Nicht in der Schweiz registrierte Unternehmungen müssen Dokumente beibringen, welche eine vergleichbare Identifikation der Wirtschaftssubjekte erlauben.

3.2.4 Antragsteller mit hohem Risiko

Swisscom Digital Certificates Services berücksichtigt Zwangsmassnamen, welche von der Schweizerischen Eidgenossenschaft erlassen werden um Sanktionen durchzusetzen. Zertfikikatsanträge von oder für natürlichen und juristischen Personen, Gruppen und Organisationen, die auf einer vom SECO publizierten Verordnung[3] bzw technisch abstützend Organisation der Vereinten Nationen (UNO)[4] aufgeführt sind, können ohne Angabe von Gründen abgelehnt werden.

3.2.5 Einzelfirma (natürliche Person)

[3] http://www.seco.admin.ch/themen/00513/00620/00622/index.html?lang=de
[4] http://www.un.org/sc/committees/1267/consolidatedlist.htm

Entfällt.
One-man business: Not supported.

3.2.6 Einfache Gesellschaft

entfällt

3.2.7 Authentifizierung einer natürlichen Person

Für die Prüfung der Identität einer natürlichen Person, die im Namen einer Organisation ein EV-Zertifikat der Zertifikatsklasse „Quartz" beantragt, sind folgende Schritte durchzuführen:

1. Der Antragsteller eines Zertifikats wird persönlich bei der zuständigen RA vorstellig und legt für die Identitätsprüfung eines oder mehrere amtliche Ausweispapiere mit Lichtbild (Identitätskarte, Reisepass, Meldebescheinigung des Einwohnermeldeamts) vor.
2. Ein Mitarbeiter der RA führt die Identitätsprüfung anhand eines oder mehreren amtlichen Ausweispapieren mit Lichtbild (Identitätskarte, Reisepass, Meldebescheinigung des Einwohnermeldeamts) durch und dokumentiert das Verfahren. Der RA-Vertragspartner (E-RA/TSP) muss über einen gültigen RA-Partnervertrag mit Swisscom Solution verfügen.
3. Für alle im Zertifikat vermerkten Attribute haben ein Nachweis und eine Bestätigung anhand eines amtlichen Dokuments zu erfolgen.

Verfügt der Antragsteller bereits über ein gültiges Zertifikat, kann die Beantragung weiterer Zertifikate für diese Person auch durch die Übersendung eines verschlüsselten und unterzeichneten Antrags erfolgen, sofern sich die Identität der betreffenden 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 die bei der Identifizierung vorgelegten Ausweisdokumente noch gültig sind.

3.2.8 Überprüfung des Domain-Namens des Antragstellers

English Translation see 10.1 (3.2.3 Economic Subject with excerpt from the commercial register).

Swisscom Digital Certificate Services überprüft den Domain-Namen des Antragstellers über eine Whois-Abfrage. Der Antragsteller muss für die Beantragung eines EV-Zertifikats ein Bestätigungsschreiben vorlegen, das vom technischen Kontakt des Whois-Auszugs unterzeichnet ist.
Ist der Domain-Name des Antragstellers nicht verzeichnet, ähnelt aber dem Namen einer bekannten Domäne, werden die von der Anti-Phishing Work Group erstellten Namenslisten mit potenziellen Phishing-Angriffszielen überprüft.
Es werden ausschliesslich Zertifikate ausgestellt, für welche eine Legimitation oder Kontrolle vorliegt – im speziellen werden keine Man-In-The-Middle-Zertifikate ausgestellt.

3.2.9 Überprüfung der E-Mail Adresse des Antragsstellers

English Translation see 10.3 (3.2.9 Checking the e-mail address of the applicant)

Der Antragsteller muss nachweisen, dass er Zugang zu der Mailbox hat und dass er sie verwenden kann, um Mails zu empfangen.

3.2.10 Nicht überprüfte Informationen

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

3.2.11 Überprüfung der Unterschriftenvollmacht

Für einen Zertifikatsantrag für eine Organisation oder juristische Person muss der Antragsteller eine rechtsgültige und unterzeichnete Vollmacht der Organisation oder juristischen Person vorweisen.

3.2.12 Cross-Zertifizierung

Eine Cross-Zertifizierung wird momentan von Swisscom für den Service nicht angeboten.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

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 unveränderten Inhaltsdaten. In [RFC 3647] wird dieser Vorgang „certificate re-key“ genannt.

3.3.1 Routinemässige Zertifikatserneuerung (re-key)

Eine routinemässige Zertifikatserneuerung setzt voraus, dass der Zertifikatsinhaber über ein gültiges Zertifikat der zuständigen CA (Zertifikatsklasse „Quartz“) verfügt. Dazu sollte der Zertifikatsinhaber den Antrag auf ein neues Zertifikat vor Ablauf der Gültigkeit des zu erneuernden Zertifikats 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 beim Neuantrag (3.2) zu verfahren.

3.3.2 Zertifikatserneuerung 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 bei der CSP oder der zuständigen RA für ungültig erklären zu können, wird dem Zertifikatsinhaber oder die juristische 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 schriftlich erfolgen. Unter bestimmten Voraussetzungen kann eine Ungültigerklärung auch elektronisch über das Webportal der CSP erfolgen. Einzelheiten sind Abschnitt 3.4 der CPS [8] zu entnehmen.
Für eine Ungültigerklärung gelten folgende Zuständigkeiten:

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

4 Betriebsanforderungen für den Lebenszyklus von Zertifikaten

Swisscom Digital Certificate Services stellt sicher, dass an der Bearbeitung und Genehmigung von EV-Zertifikatsanträgen mindestens zwei vertrauenswürdige Personen beteiligt sind, bevor das EV-Zertifikat ausgestellt wird.

4.1 Zertifikatsanträge

4.1.1 Annahme von Zertifikatsanträgen

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

4.1.2 Registrierungsprozess

Ein Zertifikat kann durch die Zertifizierungsstelle erst erstellt werden, wenn der Registrierungsprozess bei der Registrierungsstelle eines RA-Vertragspartners erfolgreich abgeschlossen wurde. Die Dokumentation des Registrierungsprozesses bei natürlichen Personen beinhaltet zumindest:

- Zertifikatsantrag
- Kopien aller vorgelegter Ausweisdokumente mit einem aktuellen Lichtbild
- Bestätigung des Antragstellers eines Zertifikats, den Kundenvertrag (mit allen Bestandteilen wie Leistungsbeschreibung, Nutzungsbedingungen und den allgemeinen Geschäftsbedingungen) 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 des Zertifikatsantrags

4.2.1 Durchführung der Identifikation und Authentifizierung

Die zuständige Registrierungsstelle des RA-Vertragspartners führt die Identifikation und Authentifizierung eines Antragstellers eines Zertifikats nach den in Abschnitt 3.2 genannten Verfahren durch.

4.2.2 Annahme oder Abweisung von Zertifikatsanträgen

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

- Der Zertifikatsinhabervertrag muss von einer zeichnungsberechtigten Person unterschrieben werden[5]. Die den Vertrag unterzeichnende Person muss nach Abschnitt 3.2.2 authentifiziert sein.
- Der Antrag auf ein EV-Zertifikat muss von dem Antragsteller eines Zertifikats unterschrieben sein, der das Dokument vorlegt. Wenn der Antragsteller eines Zertifikats nicht gleichzeitig berechtigt ist, den Zertifikatsantrag zu genehmigen, muss eine unabhängige Person, die hierfür

[5] Diese Person KANN vom Antragsteller berechtigt worden sein, eine, zwei oder alle drei der Rollen (Vertragsunterzeichnende Person, Antragstellende Person, den Antrag genehmigende Person) zu übernehmen, sofern die Person, die den Zertifikatsantrag genehmigt und die Person, die den Vertrag unterzeichnet, in jedem Fall Angestellte des Antragstellers sind. Ein Antragsteller KANN zudem einer oder mehreren Personen die Berechtigung zur Übernahme der einzelnen Rollen erteilen.

berechtigt ist, den EV-Zertifikatsantrag genehmigt haben. Der Antragsteller eines Zertifikats und die Person, die den Zertifikatsantrag genehmigt, sind gemäss Abschnitt 3.2.2 authentifiziert.
- Es wurden alle notwendigen Dokumente vorgelegt (siehe Abschnitt 4.1.2)
- Es wurden alle ggf. festgelegten Gebühren bezahlt (siehe Abschnitt 9.1).

Nach erfolgreicher Prüfung der oben genannten Kriterien und nach Durchführung der Identifikation und Authentifizierung wird der Zertifikatsantrag durch die Zertifizierungsstelle weiter bearbeitet. Sollte die Prüfung der oben genannten Kriterien oder die Identifikation und Authentifizierung eines Antragstellers eines Zertifikats nicht erfolgreich sein, wird der Zertifikatsantrag 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]** unter 4.2.3 zu entnehmen.

4.3 Zertifikatsausstellung
Nach Eingang und erfolgreicher Prüfung (siehe 4.2.2) eines Zertifikatsantrags
- das nicht SSCD basierte Zertifikat ohne privaten Schlüssel wird entweder direkt dem Antragsteller ausgehändigt oder über einen sicheren Weg geliefert.
- stellt der Certificate Service Provider (CSP) ein EV-Zertifikat der Zertifikatsklasse „Quartz“ aus.
- wird der Antragsteller über diesen Vorgang informiert (siehe 4.3.2).
- wird das Dokument mit den Nutzungsbedingungen und 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 Zertifikatsausstellung wird dem Antragsteller eines Zertifikats das ausgestellte Zertifikat in geeigneter Weise übermittelt. Die Verfahren sind der Aussage über die Zertifizierungspraxen [2] unter 4.3 zu entnehmen.

4.4 Zertifikatsakzeptanz
Der Zertifikatsinhaber ist verpflichtet, die Korrektheit des eigenen Zertifikats sowie des Zertifikats der Zertifizierungsstelle nach Erhalt zu verifizieren.

4.4.1 Annahme des Zertifikats
Ein Zertifikat wird durch den Zertifikatsinhaber akzeptiert, wenn
- das Zertifikat verwendet wird oder
- eine explizite Äusserung erfolgt oder
- wenn innerhalb eines in der Aussage über die Zertifizierungspraxen [2] unter Abschnitt 4.4.1 festgelegten Zeitraums kein Widerspruch erfolgt.

Fehlerhaft ausgestellte Zertifikate hat die ausstellende Registrierungsstelle unverzüglich bei der zuständigen Registrierungsstelle oder bei der CSP 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 Zertifizierungspolitik ausgestellten Zertifikate ist dem Abschnitt 1.4 zu entnehmen. EV-Zertifikate der Zertifikatsklasse „Quartz" können von den Zertifikatsinhabern als SSL/TLS-Web-Server-Zertifikat verwendet werden, um die Verbindung eines Clients (Webbrowser, webbasierte Anwendung usw.) mit dem Webserver (Webserver, Webservice usw.) sicherzustellen.

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber

Durch Annahme des Zertifikats versichert der Zertifikatsinhaber allen Teilnehmern von Swisscom Digital Certificate Services und allen Parteien, die sich auf die Vertrauenswürdigkeit der in dem Zertifikat enthaltenen Informationen verlassen, dass:

- ein angemessenes Verständnis der Anwendung und des Einsatzes von Zertifikaten besteht,
- sämtliche Angaben und Erklärungen des Zertifikatsinhabers 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 Zertifizierungspolitik eingesetzt wird,
- das Zertifikat unverzüglich ungültig erklärt wird, wenn die Angaben des Zertifikats nicht mehr stimmen oder der private Schlüssel abhandenkommt, gestohlen oder möglicherweise kompromittiert wurde.

4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Zertifikatsprüfer

Jeder, der ein im Rahmen dieser Zertifizierungspolitik ausgestelltes Zertifikat zur Überprüfung der Identität eines Webservers verwendet, sollte:

- geeignete Komponenten und Verfahren zur sicheren Kommunikation mit dem Webserver einsetzen (Authentifizierung und Sitzungsverschlüsselung),
- vor der Nutzung eines Zertifikats dessen Gültigkeit überprüfen und
- das Zertifikat ausschliesslich für autorisierte und legale Zwecke in Übereinstimmung mit dieser Zertifizierungspolitik einsetzen.

4.6 Zertifikatserneuerung unter Verwendung des alten Schlüssels

Die Erstellung von neuen Zertifikaten unter Verwendung des alten Schlüssels (Zertifikatserneuerung) für EV-Zertifikate wird von Swisscom Digital Certificate Services nicht unterstützt.

4.6.1 Gründe für eine Zertifikatserneuerung

Nicht anwendbar

4.6.2 Beantragung einer Zertifikatserneuerung

Nicht anwendbar

4.6.3 Bearbeitung des Antrags auf Zertifikatserneuerung

Nicht anwendbar

4.6.4 Benachrichtigung des Zertifikatsinhabers

Nicht anwendbar

4.6.5 Annahme einer Zertifikatserneuerung
Nicht anwendbar

4.6.6 Veröffentlichung einer Zertifikatserneuerung
Nicht anwendbar

4.6.7 Benachrichtigung weiterer Instanzen über eine Zertifikatserneuerung
Nicht anwendbar

4.7 Zertifikatserneuerung unter Verwendung eines neuen Schlüssels (Re-Key)
Bei einer Zertifikatserneuerung wird grundsätzlich ein neues Schlüsselpaar erstellt. Das Zertifikat und der Schlüssel haben die gleiche Lebensdauer (i. d. R. zwei Jahre). Ein neues Zertifikat basiert immer auf einem neuen Schlüsselpaar.
Es werden die Schlüssellänge und der Algorithmus verwendet, die zu dem jeweiligen Zeitpunkt aktuell und gemäss geltender Aussage über die CPS [2] Abschnitt 7.1 einzusetzen sind. Der Zertifikatsinhaber 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 eines Re-Key
Eine Zertifikatserneuerung mit einem neuen Schlüsselpaar (Re-Key) wird grundsätzlich durch den Zertifikatsinhaber oder direkt durch den RA-Vertragspartner beantragt; es obliegt der CA zu entscheiden, ob sie eine Zertifikatserneuerung aktiv unterstützt. Die entsprechenden Verfahren sind der Aussage über die CPS [2] unter 4.6.2 zu entnehmen.

4.7.3 Ablauf Re-Key
Der Ablauf der Zertifikatserneuerung mit einem neuen Schlüsselpaar (Re-Key) entspricht den Regelungen unter 4.3; für die Identifizierung und Authentifizierung bei der erneuten Zertifizierung gelten die Regelungen gemäss Abschnitt 3.3.1.

4.7.4 Benachrichtigung des Zertifikatsinhabers bei Re-Key
Es gelten die Regelungen aus Abschnitt 4.3.2.

4.7.5 Annahme eines Re-Key
Es gelten die Regelungen aus Abschnitt 4.4.1.

4.7.6 Veröffentlichung bei Re-Key
Es gelten die Regelungen aus Abschnitt 4.4.2.

4.7.7 Benachrichtigung weiterer Instanzen bei Re-Key

Es gelten die Regelungen aus Abschnitt 4.4.3.

4.8 Zertifikatsmodifizierung

Bei der Zertifikatsmodifizierung wird aufgrund von Veränderungen der Informationen im Zertifikat ein neues Zertifikat mit demselben Schlüsselpaar erstellt. Hat sich die Identität des Zertifikatsinhabers geändert, ist wie bei einem Neuantrag zu verfahren. Das alte Zertifikat wird nach Ausstellung des neuen Zertifikats ungültig erklärt.
Zertifikatsmodifizierungen werden nur dann ausgeführt, wenn das zugehörige Schlüsselpaar noch mindestens 12 Monate gültig ist und sich die Identität des Zertifikatsinhabers nicht geändert hat. Ist dies nicht der Fall, wird eine Zertifikatserneuerung mit einem neuen Schlüsselpaar (Re-Key) vorgenommen.

4.8.1 Gründe für eine Zertifikatsmodifizierung

Gründe für eine Zertifikatserneuerung sind:

- Schreibfehler bei der Ausstellung des Zertifikats
- Änderungen der im Zertifikat enthaltenen Informationen, so z. B. geänderte Firmennamen oder geänderte URL-Adressen

4.8.2 Beantragung einer Zertifikatsmodifizierung

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

4.8.3 Bearbeitung von Anträgen auf Zertifikatsmodifikation

Der Ablauf der Zertifikatserneuerung entspricht den Regelungen unter 4.3; für die Identifikation und Authentifizierung bei der Zertifikatsmodifizierung gelten die Regelungen gemäss Abschnitt 3.3.1.

4.8.4 Benachrichtigung des Zertifikatsinhabers 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 aus Abschnitt 4.4.1.

4.8.6 Veröffentlichung einer Zertifikatsmodifizierung

Es gelten die Regelungen aus Abschnitt 4.4.2.

4.8.7 Benachrichtigung weiterer Instanzen bei einer Zertifikatsmodifizierung

Es gelten die Regelungen aus 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 von Swisscom momentan nicht angeboten. Einmal ungültig erklärte Zertifikate können nicht erneuert oder verlängert werden.

4.9.1 Gründe für eine Ungültigerklärung

English Translation see 10.3 (3.2.9 Checking the e-mail address of the applicant).

Zertifikate müssen von der zuständigen Registrierungsstelle oder dem Certificate Service Provider ungültig erklärt werden, wenn:

1. der Zertifikatsinhaber oder die juristische Person oder Organisation, die diesen vertritt, einen entsprechenden Antrag stellt
2. der Zertifikatsinhaber meldet, dass der ursprüngliche Antrag auf ein EV-Zertifikat nicht autorisiert war und er keine rückwirkende Autorisierung erteilt
3. die Zertifizierungsstelle nach eigenem Ermessen feststellt, dass das EV-Zertifikat nicht im Einklang mit den Bedingungen dieser Richtlinien oder den Regelungen der Zertifizierungsstelle ausgestellt wurde.
4. dem Certificate Service Provider oder der Registrierungsstelle mindestens einer der folgenden Gründe bekannt ist:
    - Ein Zertifikat enthält Angaben, die nicht (mehr) gültig sind.
    - Das Zertifikat ist unrechtmässig erlangt worden.
    - Das Zertifikat bietet keine Gewähr mehr für die Zuordnung eines Signaturprüfschlüssels zu einer bestimmten Organisation oder juristischen Person.
    - Der private Schlüssel des Zertifikatsinhabers wurde geändert, verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
    - Der Zertifikatsinhaber hat seine Berechtigungsgrundlage verloren (siehe Abschnitt 1.3.3).
    - Der Zertifikatsinhaber ist nicht länger der rechtmässige Eigentümer des Domainnamens (siehe Abschnitt 3.2.4)
    - Der Zertifikatsinhaber richtet sich nicht nach dieser Zertifizierungspolitik.
    - Die zuständige Registrierungsstelle richtet sich nicht nach dieser Zertifizierungspolitik oder nach der Aussage über die CPS [2].
    - Der Zertifikatsinhaber benötigt das betroffene Zertifikat nicht mehr.
    - Der Zertifikatsbetrieb wird eingestellt.
    - Der Zertifikatsinhaber kommt seiner Zahlungspflicht auch nach mehrmaliger Aufforderung nicht nach.
    - Der Zertifikatsinhaber verletzt eine der wesentlichen Pflichten, die aus dem Zertifikatsinhabervertrag entstehen.
    - Die im EV-Zertifikat enthaltenen Informationen haben sich entscheidend geändert.
    - Der Zertifikatsinhaber wurde als gesperrte Partei oder Person einer schwarzen Liste hinzugefügt oder hat seinen Geschäftssitz an einem Ort, der gemäss der rechtlichen Vorschriften der Zertifizierungsstelle bezüglich des Geschäftsbetriebs (siehe Abschnitt 23 der EV-Zertifikatsrichtlinien) als Geschäftssitz unzulässig ist.

4.9.2 Wer kann die Ungültigkeitserklärung vornehmen

Zertifikate können grundsätzlich nur von der ausstellenden Registrierungsstelle (dem RA-Vertragspartner) oder der Zertifizierungsstelle ungültig erklärt werden. Jeder Zertifikatsinhaber kann bei der zuständigen Registrierungsstelle, die sein Zertifikat erstellt hat, beantragen, dass diese ein für ihn ausgestelltes Zertifikat ungültig erklärt. Verfahrensanweisungen für die Ungültigkeitserklärung sind der entsprechenden Aussage über die Zertifizierungspraxen [2] unter 4.9 zu entnehmen. Voraussetzung für die Akzeptanz einer Ungültigkeitserklärung eines Zertifikats ist eine erfolgreiche Identifizierung und Authentifizierung des Zertifikatsinhabers entsprechend Abschnitt 3.4.

4.9.3 Ablauf einer Ungültigkeitserklärung eines Zertifikats

Sind die Voraussetzungen für eine Ungültigkeitserklärung eines Zertifikats erfüllt, wird das Zertifikat unverzüglich gesperrt.
Der Zertifikatsinhaber wird über die Ungültigkeitserklärung umgehend informiert.

4.9.4 Fristen für den Zertifikatsinhaber

Der Zertifikatsinhaber muss unverzüglich die zuständige Registrierungsstelle oder den Certificate Service Provider benachrichtigen und die Ungültigkeitserklärung des eigenen Zertifikats veranlassen, wenn Gründe (siehe 4.9.1) für eine Ungültigkeitserklärung vorliegen. Der Certificate Service Provider bietet auf seinem Webportal einen entsprechenden Dienst an, um auch ausserhalb der Geschäftszeiten der Registrierungsstelle Anträge auf Ungültigkeitserklärung entgegennehmen zu können.

4.9.5 Zeitrahmen der Zertifizierungsstelle für die Bearbeitung von Anträgen auf Ungültigkeitserklärung

Die Registrierungsstelle (der RA-Vertragspartner) soll einen Antrag auf Ungültigkeitserklärung unverzüglich bearbeiten, wenn die oben genannten Voraussetzungen gegeben sind.

4.9.6 Anforderungen zur Kontrolle der Zertifikatssperrliste (CRL) durch den Zertifikatsprüfer

Es gelten die Regelungen aus Abschnitt 4.5.2.

4.9.7 Aktualisierungsintervall der Zertifikatssperrlisten

Das Aktualisierungsintervall für eine Zertifikatssperrliste ist der entsprechenden Aussage über die Zertifizierungspraxen [2] unter 4.9.7 zu entnehmen. Die Zertifikatssperrliste wird jedoch mindestens alle 24 Stunden aktualisiert.

4.9.8 Maximale Latenzzeit für Zertifikatssperrlisten

Die maximale Latenzzeit für eine Zertifikatssperrliste ist der entsprechenden Aussage über die Zertifizierungspraxen [2] unter 4.9.7 zu entnehmen.

4.9.9 Verfügbarkeit von Online-Verfahren zur Ungültigkeitserklärung/Status-Überprüfung

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. Detailinformationen sind der entsprechenden Aussage über die Zertifizierungspraxen [2] unter 4.9.9 zu entnehmen.

4.9.10 Anforderungen an Online-Verfahren zur Ungültigkeitserklärung/Status-Überprüfung

Vor jeder Nutzung des Zertifikats sollte dessen Gültigkeit überprüft werden. Die Standards sind den Abschnitten 7.2 (CRL-Profil) und 7.3 (OCSP-Profil) der Aussage über die Zertifizierungspraxen [2] zu entnehmen.

4.9.11 Andere verfügbare Formen der Ungültigkeitsbekanntmachungen

Swisscom Digital Certificate Service 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 ungültig erklären zu lassen. Bei einer Kompromittierung des privaten Schlüssels einer Zertifizierungsstelle werden alle von ihr ausgestellten Zertifikate gesperrt.

4.9.13 Gründe für eine Suspendierung

Eine Suspendierung von Zertifikaten der Zertifikatsklasse „Quartz“ wird nicht angeboten.

4.9.14 Wer kann eine Suspendierung beantragen

Nicht anwendbar.

4.9.15 Ablauf eines Antrags auf Suspendierung
Nicht anwendbar.

4.9.16 Begrenzung des Suspensierungszeitraums
Nicht anwendbar.

4.10 Dienst zur Statusabfrage von Zertifikaten
Details zum Verfahren sowie zu dessen Verfügbarkeit und Merkmale sind der entsprechenden Aussage über die Zertifizierungspraxen [2] unter 4.10 zu entnehmen. Der Dienst steht normalerweise rund um die Uhr zur Verfügung.

4.10.1 Verfahrensmerkmale
Die Verfahrensmerkmale sind dem CPS **[8]** unter 4.10.1 zu entnehmen.
Verfügbarkeit des Dienstes
Die Angaben über die Verfügbarkeit des Dienstes sind der der Aussage über die Zertifizierungspraxen [2] unter 4.10.2 zu entnehmen.

4.10.2 Optionale Merkmale
Die optionalen Merkmale sind der Aussage über die Zertifizierungspraxen [2] unter 4.10.3 zu entnehmen.

4.11 Beendigung des Vertragsverhältnisses durch den Zertifikatsinhaber
Die Dauer des Vertragsverhältnisses ergibt sich aus der im Zertifikat angegebenen Gültigkeitsdauer (i. d. R. 2 Jahr).
Die Aufbewahrungsdauer von Dokumenten und Zertifikaten beträgt 7 Jahre und wird durch den Certificate Service Provider sichergestellt.

4.12 Schlüsselhinterlegung und -wiederherstellung
Schlüsselhinterlegung und -wiederherstellung (Key escrow and recovery) wird für fortgeschrittene Signaturschlüssel der Zertifikatsklasse „Quartz“ derzeit nicht angeboten. Das Schlüsselpaar wird durch den Kunden erstellt, weswegen Swisscom als Certificate Service Provider keine Möglichkeit hat, private Schlüssel wiederherzustellen.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen

Weitere Informationen zu infrastrukturellen, organisatorischen und personellen Sicherheitsmassnahmen sind dem Anhang der CPS [8] zu entnehmen.

6 Technische Sicherheitsmassnahmen

Technische Sicherheitsmassnahmen sind Paragraf 6 der CPS [8] zu entnehmen.

7 Profile für Zertifikate

Die Profile der Zertifikate entsprechen den Richtlinien des CA/Browser-Forums für die Ausstellung und Verwaltung von Extended-Validation-Zertifikaten („Guidelines for the Issuance and Management of Extended Validation Certificates“, Version 1) [9].

7.1 Zertifikatprofil

Die Details des Zertifikatsprofils sind dem CPS **[8]** unter 7.1 zu entnehmen.

Zertifikaterweiterungen

Die Details der Zertifikatsprofilerweiterung sind dem CPS **[8]** unter 7.1 zu entnehmen.

7.2 CRL Profile

7.2.1 CRL Version

Die Details des CRL Profiles sind dem CPS **[8]** unter 7.2 zu entnehmen.

7.2.2 CRL Erweiterungen

Die Details zu CRL Erweiterungen sind dem CPS **[8]** unter 7.2 zu entnehmen.

7.3 OCSP Profile

Die Details des OCSP Profile sind dem CPS **[8]** unter 7.3 zu entnehmen.

8 Konformitätsprüfung (Compliance) und andere Assessments

Die CSP und die RA der RA-Vertragspartner, die EV-Zertifikate ausstellen, sind verpflichtet, alle ihre Abläufe dieser CP und der CPS [8] entsprechend zu gestalten.

8.1 Intervall und Umstände der Überprüfung

Da sich die CA in die Prozesse und physikalische Infrastruktur der nach ZertES zertifizierten Umgebung 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", Absatz c und d verpflichtet jährlich eine Überprüfung einer internen Kontrollstelle (internes Audit) durchzuführen. Integrierter Bestandteil dieser Prüfung ist auch die RA und die E-RA/TPS der RA Vertragspartner.

8.2 Identität und Qualifikation der Überprüferin

Die erstmalige und 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 (http://www.sas.ch/de/sas-index.html) in der Rubrik „Akkreditierte Stellen" abrufbar.
Die Funktion der internen Revision wird durch eine kompetente externe Unternehmung 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 CISO der Swisscom 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 von Swisscom Digital Certificate Services oder der vom RA-Vertragspartner geführten CA erbracht werden, sind in einer Preisliste aufgeführt, die bei der unter Abschnitt 1.5 angegebenen Kontaktadresse angefordert werden kann. Zusätzliche Leistungen, die nicht in der Preisliste aufgeführt 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 Geschäftsdaten

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 sowie alle Informationen, die während des Registrierungsprozesses kommuniziert wurden.

9.3.2 Nicht vertraulich zu behandelnde Daten

Jegliche Informationen, die in den ausgestellten Zertifikaten und der CRL explizit (z. B. Elemente des DN, E-Mail-Adressen) 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 CA trägt Swisscom 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 die CA weitergeben oder Daten von der CA 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

Im Umgang mit Personendaten hält sich die CA an die geltende Gesetzgebung, insbesondere an das Fernmeldegesetz (FMG) und das Bundesgesetz über den Datenschutz (DSG). Die CA 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) müssen gemäss den Bestimmungen aus Artikel 14 ZertES [1] erfüllt werden.

9.4.1 Nicht vertraulich zu behandelnde Personendaten

Entfällt.

9.4.2 Verantwortlicher Umgang mit Personendaten

Swisscom und die von ihr beauftragten RA sind dazu verpflichtet, sich im Umgang mit Personendaten an das Bundesgesetz über den Datenschutz und das Fernmeldegesetz (FMG) zu halten.
Personendaten dürfen nur rechtmässig beschafft werden. Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.
Personendaten dürfen nur zu dem bei der Beschaffung angegeben Zweck und gemäss den gesetzlichen Bestimmungen (Artikel 4 DSG) bearbeitet werden.
Personendaten dürfen nicht für kommerzielle Zwecke verwendet werden (Artikel 14 Abschnitt 1 ZertES [1]).

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
- zugehörige CPS [8]
- Markenrechte, insbesondere an Swisscom Digital Certificate Services, sowie an den weiteren Vertragsdokumenten.

Swisscom räumt den RA-Vertragspartnern und den Zertifikatsinhabern das Recht ein, die genannten Dokumente unverändert an Dritte weiterzugeben. Weitergehende Rechte werden nicht eingeräumt. Insbesondere die Weitergabe veränderter Fassungen und die Überführung in andere Dokumente oder Publikationen ohne schriftliche Zustimmung von Swisscom sind nicht zulässig.

9.6 Zusicherung und Gewährleistung

9.6.1 Verpflichtung der Zertifizierungsstellen

Swisscom verpflichtet sich als CA zur Ausführung aller im Rahmen dieser CP und der zugehörigen CPS [8] beschriebenen Aufgaben zur Anwendung der Bestimmungen gemäss ZertES und sämtlichen anderen Anwendungsbestimmungen (TAV [3]) durchzuführen.

9.6.2 Verpflichtung der RA-Vertragspartner und Registrierungsstellen

Das Geschäftsmodell von Swisscom Digital Certificate Services sieht ein RA-Vertragspartnermodell vor. Dabei übernehmen Vertragspartner die Funktion der RA. So soll sichergestellt werden, dass

- die angebotenen Zertifikate optimal in die entsprechenden Anwendungen des RA-Vertragspartners integriert sind;
- der Antragsteller auf möglichst einfache Weise ein Zertifikat erhält;
- Zertifikate der Swisscom Digital Certificate Services von verschiedenen Dienstanbietern verwendet werden können.

Die RA-Vertragspartner sind vertraglich verpflichtet, alle Anforderungen gemäss ZertES [1] und 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 der zugehörigen CPS [8] beschriebenen Aufgaben und Verpflichtungen wahrzunehmen.

9.6.3 Verpflichtung der Zertifikatsinhaber
Es gelten die Regelungen in Abschnitt 4.5.1.

9.6.4 Verpflichtung des Zertifikatsprüfer
Es gelten die Regelungen in Abschnitt 4.5.2.

9.6.5 Verpflichtung anderer Teilnehmer
Sofern weitere Teilnehmer als Dienstleister in den Zertifizierungsprozess eingebunden werden, ist Swisscom 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 dem Inhaber und Drittpersonen, die sich auf ein gültiges Zertifikat verlassen, für Schäden, welche diese erleiden, weil Swisscom (Schweiz) AG diesen Pflichten nicht nachgekommen ist. Die Haftungssumme ist auf CHF 10‘000.- pro Schadensfall begrenzt.

Swisscom (Schweiz) AG haftet nicht für Schäden, die sich aus der Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung im Zertifikat ergeben. In keinem Fall haftet Swisscom (Schweiz) AG für Folgeschäden, entgangenen Gewinn und Datenverluste.

Swisscom (Schweiz) AG haftet nicht für Schäden und Verzugsfolgen, die durch höhere Gewalt, Naturereignisse (z.B. Blitzschlag, Elementarereignisse), Stromversorgungsausfälle, kriegerische Ereignisse, Streik, unvorhersehbare behördliche Restriktionen, Umgehung von Sperrsets, PC-Dialer, Hackerattacken, Virenbefall (inkl. trojanische Pferde u.ä.) von Datenverarbeitungsanlagen usw. entstehen. 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 Nutzungsbedingungen 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 neuere Version ersetzt wird oder
- der Betrieb der CA der Swisscom Digital Certificate Services eingestellt wird.

9.10.3 Konsequenzen der Aufhebung
Von einer Aufhebung der CP und der zugehörigen CPS [8] bleibt die Verantwortung zum Schutz vertraulicher Daten und Personendaten sowie jegliche darüber hinaus bestehenden Pflichten der Parteien unberührt.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern
Die CA kommuniziert mit dem Zertifikatsinhaber via signierter E-Mail (sofern E-Mail-Adresse bekannt) oder Briefpost.
Die Kommunikation mit den übrigen Teilnehmern erfolgt mittels signierten Formularen via E-Mail oder Briefpost. Ankündigungen und News werden auf der Homepage von Swisscom veröffentlicht.

9.12 Änderungen der Zertifizierungspolitik

Für die CP und sämtliche Änderungen derselben besteht ein formelles Genehmigungsverfahren.

9.13 Konfliktbeilegung
Alle sich aus der vorliegenden CP ergebenden Streitigkeiten, an denen Swisscom beteiligt ist, sind gemäss den Bestimmungen des Konkordats über die Schiedsgerichtsbarkeit einem Dreierschiedsgericht mit Sitz in Bern zur endgültigen Entscheidung vorzulegen. 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, um den Streit einvernehmlich beizulegen. Dazu können sie einen gemeinsam ausgewählten Vermittler hinzuziehen.

Ein solcher Vermittlungsversuch hat keine Auswirkungen auf gesetzliche Verjährungsfristen.

9.14 Anwendbares Recht und Gerichtsstand

Die CP der Swisscom Digital Certificate Services unterliegt der schweizerischen Gesetzgebung. Ausschliesslicher Gerichtsstand ist Bern (Schweiz).

9.15 Konformität mit dem anwendbaren Recht

Swisscom behält sich das Recht vor, im Sinne des schweizerischen Signaturgesetzes (ZertES [1]) als CA zu handeln und qualifizierte Zertifikate auszustellen. Es werden Zertifikate ausgestellt, mit denen qualifizierte elektronische Signaturen gemäss dem schweizerischen Signaturgesetz erzeugt werden können. Diese sind gemäss OR Artikel 14 Absatz 2 von Gesetzes wegen der eigenhändigen Unterschrift gleichgestellt.

9.16 Weitere Bestimmungen

9.16.1 Geltungsbereich

Alle in der CP und der CPS [8] enthaltenen Regelungen gelten für die CA der Swisscom Digital Certificate Services und den jeweiligen Inhaber von Zertifikaten, die auf dieser CP basieren. Die Veröffentlichung einer neuen Fassung ersetzt alle vorherigen Fassungen. Mündliche Absprachen und Nebenabsprachen sind nicht zulässig.

9.16.2 Sprache

Um die internationale Zusammenarbeit mit anderen Zertifizierungsstellen zu ermöglichen, werden ggf 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

Entfällt

9.16.5 Übertragung der Rechten und Pflichten

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

10 Appendix: Translation from elected section in English

10.1 3.2.3 Economic Subject with excerpt from the commercial register

Companies listed in the commercial register are checked based on the excerpt from the commercial register that the organization actually exists and which persons are authorized to sign for that organization. The document submitted must be certified and must not be older than one year.
To obtain an EV certificate a company has to be in one of the following countries in the Commercial Register:

- Switzerland

Companies not registered in Switzerland must submit documentations that allow comparable identification of the company.

10.2 3.2.8 Checking the domain name of the applicant

Swisscom Digital Certificate Services checks the domain name of the applicant via a Whois query. The applicant must submit for an EV certificate request a written confirmation signed by the technical contact of the Whois statement.
In case the domain name of the applicant is not listed, but looks similar to the name of a known domain then the name lists of potential phishing attack targets maintained by the Anti-Phishing Workgroup are tested.

10.3 3.2.9 Checking the e-mail address of the applicant

The requester must prove that he has accessto the mailbox and that he can use it to receive mail.

10.4 4.9.1 Circumstances for revocation

Zertifikate müssen von der zuständigen Registrierungsstelle oder dem Certificate Service Provider ungültig erklärt werden, wenn:
Certificates have to be revoked by the appropriate registration authority or the Certificate Service Provider if:

1. the certificate holder or the legal person or organization that represents it, makes an revocation application
2. the certificate holder reports that the original EV certificate application was not authorized and he does not give retroactive authorization
3. the certification authority determines in its discretion, that the EV Certificate was not issued in accordance with the terms of this Policy or the provisions of the CA.
4. the Certificate Service Provider or the registrar knows at least one of the following facts.
    - A certificate contains information that is not valid (more)
    - The certificate has been obtained unlawfully.
    - The certificate does no longer guarantee that the assignment of a signature verification key to a specific organization or entity.
    - The private key of the certificate holder has been changed, lost, stolen, disclosed or otherwise compromised or abused.
    - The certificate holder has lost his entitlement basis
    - The certificate holder is no longer the legal owner of the domain name
    - The certificate holder is not compliant with this certification policy
    - The competent registration authority is not compliant with this certification policy or after the statement about the CPS
    - The certificate holder performs Code Signing for malware (such as viruses,

Trojans and spyware).

- The information contained in the EV Certificate have crucially changed.