Swisscom Digital Certificate Services

Certificate Policy (CP)

Zertifikatsklasse „Rubin“

Zusammenfassung	Certificate Policy für Zertifikate der Klasse Rubin der Swisscom Digital Certificate Services, einer Dienstleistung der Swisscom (Schweiz) AG zur Ausgabe von digitalen Zertifikaten für die Erstellung von elektronischen Signaturen, zur Authentisierung und Verschlüsselung.
Name	009_cp_rubin_2_16_756_1_83_v2.4.doc
Version	2.4.
Klassifizierung	Nicht klassifiziert
OID der CP	2.16.756.1.83.4 (Rubin CA 1) 2.16.756.1.83.14.0 (Rubin CA 2) 2.16.756.1.83.22.0 (Rubin CA 3)
Zugehöriges CPS	CPS Swisscom Digital Certificate Services (OID: 2.16.756.1.83.2.1)
Name der CA	Swisscom Rubin CA 1 (OID 2.16.756.1.83.4) Swisscom Rubin CA 2 (OID 2.16.756.1.83.14) Swisscom Rubin CA 3 (OID 2.16.756.1.83.22)
Inhaber der CA	Swisscom (Schweiz) AG
Sprache	Deutsch (rechtlich verbindliche Originalversion)
Beginn der CP-Konformitätsprüfung	14. April 2006 (Rubin CA 1) 1. Januar 2011 (Rubin CA 2) 1. Oktober 2014 (Rubin CA3)
Dokumenten Freigabe	Governance Board der Swisscom Digital Certificate Services

2.0	10.01.2012	Governance Board	Freigabe durch Ausschuss
2.1	22.03.2012	Hans-Peter Waldegger	Anpassungen Feedback KPMG zu ETSI 102 042
2.1	02.04.2012	Governance Board	Freigabe durch den Ausschuss
2.2	21.07.2014	Kerstin Wagner	Review und Update
2.2	25.09.2014	Governance Board	Freigabe durch den Ausschuss
2.3	02.10.2014	Patrick Graber	Ergänzung Rubin CA 3
2.4	04.06.2015	Kerstin Wagner	Review und Update
2.4	05.06.2015	Governance Board	Freigabe durch den Ausschuss

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: „Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol – OCSP“
[8]	CPS Swisscom Digital Certificate Services, OID 2.16.756.1.83.2.1
[9]	ETSI TS 102 042: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates
[10]	Addendum zum CPS [8]: Profile der Zertifikate, Sperrlisten und Online Status Anfragen

Inhaltsverzeichnis

1 EINLEITUNG 7

1.1 ÜBERBLICK 7
1.2 IDENTIFIKATION DES DOKUMENTS 8
1.3 BETEILIGTE DER SWISSCOM DIGITAL CERTIFICATE SERVICES 8
1.3.1 Zertifizierungsstellen - Certification Authorities (CA) 8
1.3.2 Registrierungsstellen – Registration Authorities (RA) 9
1.3.3 Zertifikatinhaber (Subscriber) 9
1.3.4 Zertifikatsprüfer (Relying Parties) 9
1.3.5 Weitere Teilnehmer 9
1.4 ANWENDBARKEIT DER ZERTIFIKATE (CERTIFICATE USAGE) 9
1.4.1 Geeignete Zertifikatnutzung 9
1.4.2 Untersagte Zertifikatnutzung 9
1.5 VERWALTUNG DER RICHTLINIEN 9
1.6 SCHLÜSSELWÖRTER UND BEGRIFFE 9
1.7 ABKÜRZUNGEN 10

2 VERÖFFENTLICHUNGEN UND VERANTWORTUNG FÜR DEN VERZEICHNISDIENST 11

2.1 VERZEICHNISDIENST 11
2.2 VERÖFFENTLICHUNG VON INFORMATIONEN 11
2.3 AKTUALISIERUNG DER INFORMATIONEN 11
2.4 ZUGANG ZU DEN INFORMATIONSDIENSTEN 11

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG 12

3.1 NAMEN 12
3.1.1 Namensform 12
3.1.2 Aussagekraft von Namen 12
3.1.3 Pseudonymität / Anonymität 13
3.1.4 Regeln zur Interpretation verschiedener Namensformen 13
3.1.5 Eindeutigkeit von Namen 13
3.1.6 Erkennung, Authentifizierung und Funktion von Warenzeichen 13
3.2 IDENTITÄTSÜBERPRÜFUNG BEI NEUANTRAG 13
3.2.1 Verfahren zur Überprüfung des Besitzes des privaten Schlüssels 13
3.2.2 Authentifizierung einer juristischen Person 13
3.2.3 Authentifizierung einer natürlichen Person 14
3.2.4 Nicht überprüfte Informationen 14
3.2.5 Antragsteller mit hohem Risiko 14
3.3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG BEI EINER ZERTIFIKATERNEUERUNG 14
3.3.1 Routinemässige Zertifikatserneuerung (re-key) 14
3.3.2 Zertifikaterneuerung (re-key) nach einer Ungültigerklärung 14
3.4 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG BEI EINER UNGÜLTIGERKLÄRUNG 14

4 BETRIEBSANFORDERUNGEN FÜR DEN ZERTIFIKATS LEBENSZYKLUS 15

4.1 ZERTIFIKATANTRAG 15
4.1.1 Wer kann ein Zertifikat beantragen 15
4.1.2 Registrierungsprozess 15
4.2 BEARBEITUNG DES ZERTIFIKATANTRAGS 15
4.2.1 Durchführung der Identifikation und Authentifizierung 15
4.2.2 Annahme oder Abweisung von Zertifikatanträgen 15
4.2.3 Bearbeitungsdauer 16
4.3 ZERTIFIKATAUSSTELLUNG 16

4.3.1 Weitere Prüfungen der Zertifizierungsstelle ... 16
4.3.2 Benachrichtigung des Antragstellers ... 16
4.4 ZERTIFIKATAKZEPTANZ ... 16
4.5 VERWENDUNG DES SCHLÜSSELPAARES UND DES ZERTIFIKATS ... 16
4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatinhaber ... 16
4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Zertifikatprüfer ... 17
4.6 ZERTIFIKATERNEUERUNG UNTER VERWENDUNG DES ALTEN SCHLÜSSELS (CERTIFICATE RENEWAL) ... 17
4.7 ZERTIFIKATERNEUERUNG UNTER VERWENDUNG EINES NEUEN SCHLÜSSELS (RE-KEY) ... 17
4.7.1 Gründe für Re-Key ... 17
4.7.2 Beantragung Re-Key ... 17
4.7.3 Ablauf Re-Key ... 17
4.7.4 Benachrichtigung des Zertifikatinhabers bei Re-Key ... 18
4.7.5 Annahme eines Re-Key ... 18
4.7.6 Veröffentlichung bei Re-Key ... 18
4.7.7 Benachrichtigung weiterer Instanzen bei Re-Key ... 18
4.8 ZERTIFIKATMODIFIZIERUNG ... 18
4.9 UNGÜLTIGERKLÄRUNG UND SUSPENDIERUNG VON ZERTIFIKATEN ... 18
4.9.1 Gründe für eine Ungültigerklärung ... 18
4.9.2 Wer kann die Ungültigerklärung vornehmen ... 18
4.9.3 Ablauf einer Ungültigerklärung eines Zertifikats ... 18
4.9.4 Fristen für den Zertifikatinhaber ... 19
4.9.5 Fristen für die Zertifizierungsstelle ... 19
4.9.6 Anforderungen zur Kontrolle der CRL durch den Zertifikatprüfer ... 19
4.9.7 Aktualisierung der CRL's ... 19
4.9.8 Maximale Latenzzeit für CRL's ... 19
4.9.9 Verfügbarkeit von Online-ungültigkeits-/Status-Überprüfungsverfahren ... 19
4.9.10 Anforderungen an Online-Ungültigkeits-/Status-Überprüfungsverfahren ... 19
4.9.11 Andere verfügbare Formen der Ungültigkeitsbekanntmachung ... 19
4.9.12 Kompromittierung von privaten Schlüsseln ... 19
4.9.13 Gründe für eine Suspendierung ... 19
4.9.14 Dienst zur Statusabfrage von Zertifikaten ... 19
4.9.15 Beendigung des Vertragsverhältnisses durch den Zertifikatinhaber ... 20
4.10 SCHLÜSSELHINTERLEGUNG UND -WIEDERHERSTELLUNG ... 20

5 INFRASTRUKTURELLE, ORGANISATORISCHE UND PERSONELLE SICHERHEITSMASSNAHMEN ... 20

6 TECHNISCHE SICHERHEITSMASSNAHMEN ... 20

7 PROFILE FÜR ZERTIFIKATE, WIDERRUFSLISTEN UND ONLINE-STATUSABFRAGEN ... 20

7.1 ZERTIFIKATPROFIL ... 20
7.1.1 Zertifikaterweiterungen ... 21

8 KONFORMITÄTSPRÜFUNG (COMPLIANCE AUDIT) UND ANDERE ASSESSMENTS ... 21

8.1 INTERVALL UND UMSTÄNDE DER ÜBERPRÜFUNG ... 21
8.2 IDENTITÄT UND QUALIFIKATION DER ÜBERPRÜFERIN ... 21
8.3 VERHÄLTNIS VON ÜBERPRÜFERIN ZU ÜBERPRÜFTER ... 21
8.4 ÜBERPRÜFTE BEREICHE ... 22
8.5 MÄNGELBESEITIGUNG ... 22
8.6 VERÖFFENTLICHUNG DER ERGEBNISSE ... 22

9 RAHMENVORSCHRIFTEN ... 22

9.1 GEBÜHREN ... 22
9.2 FINANZIELLE VERANTWORTUNG ... 22

9.3 SCHUTZ VON PERSONENDATEN (DATENSCHUTZ) 22
9.4 IMMATERIALGÜTERRECHTE 22
9.5 ZUSICHERUNG UND GEWÄHRLEISTUNG 22
9.6 AUSSCHLUSS DER GEWÄHRLEISTUNG 22
9.7 HAFTUNG VON SWISSCOM (SCHWEIZ) AG 23
9.8 HAFTUNG DES ZERTIFIKATINHABERS 23
9.9 INKRAFTTRETEN UND AUFHEBUNG 23
9.10 INDIVIDUELLE BENACHRICHTIGUNGEN UND KOMMUNIKATION MIT TEILNEHMERN 23
9.11 ÄNDERUNGEN DER ZERTIFIZIERUNGSRICHTLINIEN 23
9.12 KONFLIKTBEILEGUNG 23
9.13 GELTENDES RECHT UND GERICHTSSTAND 23
9.14 KONFORMITÄT MIT DEM GELTENDEN RECHT 23
9.15 WEITERE BESTIMMUNGEN 23

10 APPENDIX: ENGLISH TRANSLATION FROM SELECTED SECTIONS 24

1 Einleitung

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

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

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

Diese CP bezieht sich auf die Zertifikatklasse Rubin (Soft-Zertifikat. Für alle Zertifikate, die dieser CP entsprechen, ist der Objekt Bezeichner gemäss X.509 [OID] dieser CP im Zertifikat vermerkt. Somit wird die CP an das Zertifikat einer bestimmten Klasse gebunden.

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 und CA 3 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 Zertifikaten der Zertifikatsklasse „Rubin“ der Swisscom Digital Certificate Services
- Sicherstellung der Interoperabilität bei der Benutzung fortgeschrittener Zertifikate der Swisscom.

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]
- ETSI TS 102 042 [9]

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

1.2 Identifikation des Dokuments

Identifikation:

- Titel: Swisscom Digital Certificate Services – Certificate Policy (CP) für die Zertifikatsklasse „Rubin“
- Version: 2.4
- Object Identifier (OID) für diese CP:
  - Rubin CA 1: 2.16.756.1.83.4
  - Rubin CA 2: 2.16.756.1.83.14.0
  - Rubin CA 3: 2.16.756.1.83.22.0

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 Internetseite des BAKOM abgefragt werden (http://www.eofcom.admin.ch).

1.3 Beteiligte der Swisscom Digital Certificate Services

1.3.1 Zertifizierungsstellen - Certification Authorities (CA)

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

nur Zertifikate an natürliche Personen aus, die allerdings wiederum Vertreter einer juristischen Person oder Organisation sein können.

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

Diese CP bezieht sich nur auf eine Zertifikatsklasse, dem fortgeschrittenen digitalem Zertifikat „Rubin“ und entspricht den Anforderungen des schweizerischen Signaturgesetzes ZertES [1].

1.3.2 Registrierungsstellen – Registration Authorities (RA)

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

1.3.3 Zertifikatinhaber (Subscriber)

Ein fortgeschrittenes Zertifikat kann sowohl auf eine natürlich als auch eine juristische Person ausgestellt werden.

1.3.4 Zertifikatsprüfer (Relying Parties)

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

1.3.5 Weitere Teilnehmer

Die weiteren Teilnehmer sind im Kapitel 1.3.5 der zugehörigen CPS [8] beschrieben.

1.4 Anwendbarkeit der Zertifikate (Certificate Usage)

1.4.1 Geeignete Zertifikatnutzung

Die im Rahmen dieser CP ausgestellten Zertifikate können durch den Zertifikatinhaber für die elektronische Signatur, Authentisierung und Verschlüsselung verwendet werden.

1.4.2 Untersagte Zertifikatnutzung

Die Zertifikatsnutzung ausserhalb des in den Nutzungsvereinbarungen definierten Anwendungsbereichs ist 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] Kapitel 9.11.

1.6 Schlüsselwörter und Begriffe

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

1.7 Abkürzungen

Begriff	Erklärung
BCP	Business Continuity Plan
CA	Certification Authority
CN	Common Name, als Teil des DN
CP	Certificate Policy, Zertifizierungsrichtlinie
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
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
ISO	Information Security Officer, IT Sicherheitsverantwortlicher
LDAP	Lightweight Directory Access Protocol, Verzeichnisdienst
E-RA	Enterprise Registration Authority / 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 Authority
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)
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur

2 Veröffentlichungen und Verantwortung für den Verzeichnisdienst

2.1 Verzeichnisdienst

Swisscom stellt sicher, dass Informationen zur Überprüfung der Gültigkeit der von ihr ausgegebenen Zertifikate vom Typ Rubin CA 1 und Rubin CA 2 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 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 den Zertifikatinhabern Informationen über die Swisscom Digital Certificate Services, über die korrekte Anwendung von Kryptographie und die Verwendung von Zertifikaten 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 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.

3 Identifizierung und Authentifizierung

3.1 Namen

3.1.1 Namensform

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

Folgende Daten und Nachweise müssen erfasst werden:

Rubin (fortgeschritten),	Zu erfassende Daten
Pflicht	• Name des Zertifikatsinhabers: ○ Vorname ○ Mittelname (n) falls vorhanden ○ Nachname • Postadresse • Vorgelegtes Dokument • Gültigkeitsdauer des Dokumentes • Bevollmächtigung der juristischen Person bei Eintrag O= oder OU= im Zertifikat
Optional	• E-Mailadresse • Titel (Dr., Prof.) • Pseudonym / Acronym • OrganizationName • OrganizationalUnit • Weitere RFC konforme Attribute

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

3.1.2 Aussagekraft von Namen

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

- Zertifikate dürfen nur auf einen zulässigen Namen des Zertifikatinhabers ausgestellt werden.
- Bei der Vergabe von Namen für Firmen-, Organisations- oder Funktionszertifikate muss eine Verwechslung mit natürlichen und juristischen Personen oder Bezeichnungen von Organisationseinheiten ausgeschlossen werden. Ebenso dürfen keine DNS-Namen, IP-Adressen oder andere Syntaxelemente verwendet werden. Ein Pseudonym 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] Kapitel 3.1.2 festgelegt.

3.1.3 Pseudonymität / Anonymität

In begründeten Ausnahmen kann für eine natürliche Person anstelle des Namens im Zertifikat ein Pseudonym bzw. eine eindeutige Anonymisierung aufgeführt werden. Dieses wird bereits im CN-Feld des DN eindeutig kenntlich gemacht. Einzelheiten regelt das CPS [8] Kapitel 3.1.3. Für die Eindeutigkeit von Pseudonymen gelten weiterhin auch die Regelungen in Kapitel 3.1.5.

Die Identitätsprüfung erfolgt immer entsprechend den Regelungen unter CPS [8] Kapitel 3.2. Anonyme Zertifikate sind daher nicht möglich.

Zertifikate werden nur an juristische oder natürliche Personen ausgegeben, die ihre Identität mittels eines geeigneten Verfahrens nachweisen. Bei Firmen- oder Funktionszertifikaten kann auf Wunsch des Antragstellers der Name der natürlichen Person, welche den Signaturschlüssel kontrolliert, im Zertifikat weggelassen werden.

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 überprüft und sichergestellt werden.

3.1.6 Erkennung, Authentifizierung und Funktion von Warenzeichen

Die Regelung ist im CPS, Kapitel 3.1.6, beschrieben.

3.2 Identitätsüberprüfung bei Neuantrag

English translation see appendix 10 *„3.2 Initial identity verification“*

3.2.1 Verfahren zur Überprüfung des Besitzes des privaten Schlüssels

Der private Schlüssel wird auf der Infrastruktur des Zertifikat-Inhabers, auf der Infrastruktur des CSP oder beim RA-Vertragspartner erzeugt. 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.

3.2.3 Authentifizierung einer natürlichen Person

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

- Für alle im Zertifikat 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. 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.

3.2.4 Nicht überprüfte Informationen

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

3.2.5 Antragsteller mit hohem Risiko

Die Regelungen sind im CPS, Kapitel 3.2.5, beschrieben.

3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung

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 Zertifikaterneuerung setzt voraus, dass der Zertifikatinhaber über ein gültiges Zertifikat der zuständigen CA oder einer höherwertigeren CA Zertifikatsklasse „Saphir“ oder „Diamant“) 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 Kapitel 3.2.

3.4 Identifizierung und Authentifizierung bei einer Ungültigerklärung

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

4 Betriebsanforderungen für den Zertifikats Lebenszyklus

4.1 Zertifikatantrag

4.1.1 Wer kann ein Zertifikat beantragen

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

- natürliche Personen
- juristische Personen
- Organisationen

4.1.2 Registrierungsprozess

- Ein Zertifikat kann durch Swisscom erst erzeugt werden, wenn der Registrierungsprozess bei einem RA- oder AIS-Vertragspartner erfolgreich abgeschlossen wurde. Die Dokumentation des Registrierungsprozesseses beinhaltet zumindest:Zertifikatantrag
- Aussage darüber, ob die Informationen im Zertifikat veröffentlicht werden sollen. Standardmässig werden die Daten nicht publiziert.
  Bei Zertifikaten, die von der Rubin CA 3 ausgestellt werden, ist eine Veröffentlichung nicht möglich.

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

4.2 Bearbeitung des Zertifikatantrags

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 im Kapitel 3.2 genannten Verfahren durch.

4.2.2 Annahme oder Abweisung von Zertifikatanträgen

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

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

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

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

4.2.3 Bearbeitungsdauer

Die Bearbeitungsdauer nach Annahme des Zertifikatantrages beträgt maximal 5 Werktage.

4.3 Zertifikatausstellung

Nach Eingang und erfolgreicher Prüfung (siehe 4.2.2) eines Zertifikatantrags

- Stellt Swisscom ein fortgeschrittenes Zertifikat der Klasse „Rubin " aus
- Wird das Zertifikat dem Antragsteller ausgehändigt oder geliefert.
- Wird der Antragsteller über diesen Vorgang informiert (siehe 4.3.2).

4.3.1 Weitere Prüfungen der Zertifizierungsstelle

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

4.3.2 Benachrichtigung des Antragstellers

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

4.4 Zertifikatakzeptanz

Es gelten die Regelungen in Kapitel 4.4 der CPS.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

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

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatinhaber

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

- ein angemessenes Verständnis der Anwendung und des Einsatzes von Zertifikaten besteht,
- sämtliche Angaben und Erklärungen des Zertifikatinhabers in Bezug auf die im Zertifikat enthaltenen Informationen der Wahrheit entsprechen,
- der private Schlüssel geschützt aufbewahrt wird,
- keiner unbefugten Person Zugang zu dem privaten Schlüssel gewährt wird,
- das Zertifikat ausschliesslich in Übereinstimmung mit dieser CP eingesetzt wird,
- das Zertifikat unverzüglich ungültig erklärt wird, wenn die Angaben des Zertifikats nicht mehr stimmen oder der private Schlüssel abhanden kommt, gestohlen oder möglicherweise kompromittiert wurde.

4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Zertifikatprüfer

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

- ein grundlegendes Verständnis der Anwendung und des Einsatzes von Zertifikaten besitzen,
- geeignete Komponenten und Verfahren zur Signaturprüfung einsetzen (siehe dazu CPS [8] Kapitel 2.2)
- 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 für Zertifikate der Klasse „Rubin“ auf spezifischen Wunsch unterstützt.

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 (in der Regel 3 Jahre).

Es werden die Schlüssellänge und der Algorithmus verwendet, der zu dem jeweiligen Zeitpunkt aktuell ist und gemäss Addendum zum CPS [10] Kapitel 2.4 (CA 1) bzw. 2.11 (CA 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 der eingesetzte 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.

4.7.3 Ablauf Re-Key

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

4.7.4 Benachrichtigung des Zertifikatinhabers bei Re-Key

Es gelten die Regelungen gemäss Kapitel 4.3.2.

4.7.5 Annahme eines Re-Key

Es gelten die Regelungen gemäss Kapitel Fehler! Verweisquelle konnte nicht gefunden werden..

4.7.6 Veröffentlichung bei Re-Key

Es gelten die Regelungen gemäss Abschnitt Fehler! Verweisquelle konnte nicht gefunden werden..

4.7.7 Benachrichtigung weiterer Instanzen bei Re-Key

Es gelten die Regelungen gemäss Abschnitt Fehler! Verweisquelle konnte nicht gefunden werden..

4.8 Zertifikatmodifizierung

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

Bei einer Zertifikatsmodifizierung wird dem Zertifikatinhaber durch den zuständigen RA-Partner ein neues Zertifikat basierend auf einem neuen Schlüsselpaar ausgestellt (Re-Key-Verfahren, siehe Kapitel 4.7)

4.9 Ungültigerklärung und Suspendierung von Zertifikaten

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

4.9.1 Gründe für eine Ungültigerklärung

Zertifikate müssen von der zuständigen RA oder Swisscom ungültig erklärt werden, wennder Zertifikatsinhaber oder die juristische Person oder Organisation, die dieser vertritt einen entsprechenden Antrag stellt.

4.9.2 Wer kann die Ungültigerklärung vornehmen

Zertifikate können grundsätzlich nur von der ausstellenden RA oder von Swisscom ungültig erklärt werden. Jeder Zertifikatinhaber kann von der zuständigen RA, die sein Zertifikat erstellt hat, unter Angabe von Gründen verlangen, dass diese ein für ihn ausgestelltes Zertifikat ungültig erklärt. Verfahren für eine Ungültigerklärung eines Zertifikats sind dem zugehörigen CPS [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 widerrufen.

4.9.4 Fristen für den Zertifikatinhaber

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

4.9.5 Fristen für die Zertifizierungsstelle

Die RA bearbeitet einen Auftrag für eine Ungültigerklärung eines Zertifikats unverzüglich.

4.9.6 Anforderungen zur Kontrolle der CRL durch den Zertifikatprüfer

Es gelten die Regelungen gemäss Kapitel 4.5.2.

4.9.7 Aktualisierung der CRL's

Die CRL wird alle 2 Stunden nachgeführt.

4.9.8 Maximale Latenzzeit für CRL's

Bei einer Veränderung wird eine CRL innerhalb von 2 Stunden veröffentlicht.

4.9.9 Verfügbarkeit von Online-ungültigkeits-/Status-Überprüfungsverfahren

Swisscom bietet mehrere 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.

4.9.10 Anforderungen an Online-Ungültigkeits-/Status-Überprüfungsverfahren

Die Standards sind den Abschnitten 3 (CRL-Profil) und 4 (OCSP-Profil) des Addendums zum CPS [10] zu entnehmen.

4.9.11 Andere verfügbare Formen der Ungültigkeitsbekanntmachung

Swisscom bietet keine anderen Verfahren zur Ungültigkeitsbekannt-machung an als in Kapitel 4.10 der CPS aufgeführt.

4.9.12 Kompromittierung von privaten Schlüsseln

Bei einer Kompromittierung des privaten Schlüssels ist das entsprechende Zertifikat unverzüglich für ungültig erklären zu lassen. Bei einer Kompromittierung des privaten Schlüssels einer CA werden alle von ihr ausgestellten Zertifikate widerrufen.

4.9.13 Gründe für eine Suspendierung

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

4.9.14 Dienst zur Statusabfrage von Zertifikaten

Die Details zum Verfahren, Verfügbarkeit und dessen Merkmale sind dem CPS [8] Kapitel 4.10 zu entnehmen.

4.9.15 Beendigung des Vertragsverhältnisses durch den Zertifikatinhaber

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

4.10 Schlüsselhinterlegung und -wiederherstellung

Schlüsselhinterlegung und -Wiederherstellung (Key-Escrow and Recovery) wird für fortgeschrittene Signaturschlüssel der Stufe Rubin 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.

6 Technische Sicherheitsmassnahmen

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

7 Profile für Zertifikate, Widerrufslisten und Online-Statusabfragen

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

7.1 Zertifikatsprofil

Ein von Swisscom ausgegebenes fortgeschrittenes Zertifikat der Zertifikatsklasse „Rubin“ umfasst folgende, im X.509 v3 Standard definierten Pflichtfelder:

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

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

7.1.1 Zertifikaterweiterungen

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

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

8 Konformitätsprüfung (Compliance Audit) und andere Assessments

Swisscom und die RA-Vertragspartner, welche fortgeschrittene Zertifikate ausstellen, sind verpflichtet, alle ihre Abläufe dieser CP und dem CPS [8] entsprechend auszugestalten. Swisscom erfüllt alle Vorgaben des ZertES [1] und den 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.

8.1 Intervall und Umstände der Überprüfung

Da sich die „Rubin-CA“ in die Prozesse und physikalische Infrastruktur der nach ZertES [1] 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 RA Vertragspartner (Delegation der RA-Tätigkeit gemäss Art. 8 Abs. 4 ZertES).

8.2 Identität und Qualifikation der Überprüferin

Die jährlich wiederkehrende Konformitätsprüfung wird durch eine von Swisscom unabhängige Unternehmung durchgeführt. Nur durch die Schweizerische Akkreditierungsstelle (SAS) akkreditierte Firmen dürfen diese Prüfung durchführen. Die Liste der akkreditierten Stellen ist auf der Internetseite der SAS in der Rubrik „Akkreditierte Stellen“ abrufbar (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. Die externen und internen Auditoren sprechen sich in der Planung ab. Die Koordination erfolgt durch den ISO der

Swisscom Digital Certificate Services. Das Reporting richtet sich an die Serviceleitung und Legal & Compliance.

8.4 Überprüfte Bereiche

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

8.5 Die interne Revision erstellt in Absprache mit der Anerkennungsstelle einen Prüfplan für die Prüfhandlungen.Mängelbeseitigung

Aufgedeckte Mängel werden in Abstimmung mit der zuständigen Anerkennungsstelle und der überprüften Zertifizierungs- bzw. Registrierungsstelle zeitnah behoben. Schwerwiegende Mängel mit hohem Risiko innert 2 Wochen, alle anderen innerhalb 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 Regelungen sind dem CPS [8], Kapitel 9.1 zu entnehmen.

9.2 Finanzielle Verantwortung

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

9.3 Schutz von Personendaten (Datenschutz)

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

9.4 Immaterialgüterrechte

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

9.5 Zusicherung und Gewährleistung

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

9.6 Ausschluss der Gewährleistung

Entfällt

9.7 Haftung von Swisscom (Schweiz) AG

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

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

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

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

9.8 Haftung des Zertifikatinhabers

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

9.9 Inkrafttreten und Aufhebung

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

9.10 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

Es gibt keine Benachrichtigungen oder Kommunikation mit Inhabern von Zertifikaten der Klasse Rubin, die über die Antragstellung, Identifizierung und Authorisierung sowie die allfällige Revokation des Zertifikats hinausgeht.

9.11 Änderungen der Zertifizierungsrichtlinien

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

9.12 Konfliktbeilegung

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

9.13 Geltendes Recht und Gerichtsstand

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

9.14 Konformität mit dem geltenden Recht

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

9.15 Weitere Bestimmungen

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

10 Appendix: English Translation from selected sections

„3.2 Initial identity verification“

„3.2.1 Method to prove possession of the private key“

The private key is generated on the infrastructure of the certificate holder, the infrastructure of the Swisscom or with the RA contractor. The procedures are described in the CPS [8] section 3.2.1.

„3.2.2 Authentication of a legal entity“

Legal entities are identified by an official representative.

„3.2.3 Authentication of a natural person“

The following procedure is used for verifying the identity of natural persons requesting an advanced certificate:

- *All attributes indicated in the certificate must be proved and confirmed by an official document.*

If the applicant already has a valid certificate, and provided the person's identity has not changed, other certificates for this person can also be applied for by sending an encrypted and signed application. Prerequisite for this type of application is that no more than three years have elapsed since the initial application for the valid certificate was made and that the identification documents submitted are still valid.

„3.2.4 Non-verified information“

All information required for the identity check is examined (chapters 3.2.2 and 3.2.3). No additional information is examined.

"3.2.6 Applicants with a high risk"

Please see the related CPS, chapter 3.2.5