# Swisscom Digital Certificate Services

## Certification Practice Statement (CPS)

Für die:

- Swisscom Root CA 2 (OID 2.16.756.1.83.10.0)
- Issuing CA's (Diamant, Saphir, Rubin, Smaragd, Time-Stamping)

| | |
|---|---|
| Zusammenfassung | Certification Practice Statement für Zertifikate der Swisscom Digital Certificate Services zur Ausgabe von digitalen Zertifikaten zur Erstellung von qualifizierten und fortgeschrittenen elektronischen Signaturen gemäss ZertES. |
| Name | CPS_SDCS_2_16_756_1_83_2_1 |
| Version | 2.13 |
| Freigabe | 10.10.2017 |
| Ablauf | 28.02.2018 (Ersatz durch CP/CPS_Diamant_Saphir_v3.0) |
| Klassifikation | Public |
| OID dieser CPS | 2.16.756.1.83.2.1 |
| Namen der CA's | Swisscom Root CA 2,<br>- Diamant CA 2,<br>- Saphir CA 2,<br>- Rubin CA 2, Rubin CA 3<br>- Smaragd CA 2,<br>- Time-Stamping CA 2 |
| Inhaber der CA | Swisscom (Schweiz) AG |
| Sprache | Deutsch (rechtlich verbindliche Originalversion) |
| Beginn der CP/CPS Konformitätsüberprüfung | 1. Januar 2011 (Swisscom Root CA 2) |
| Dokumenten Freigabe | Governance Board der Swisscom Digital Certificate Services |

## Änderungskontrolle

| Version | Datum | Ausführende Stelle | Bemerkungen/Art der Änderung |
|---|---|---|---|
| 2.0 | 15.06.2011 | H.P. Waldegger | Neue CA 2 Hierarchie und Details für Root eingefügt. |
| 2.1 | 01.12.2011 | Markus Limacher | Update CA 2 Hierarchie; update CA 2 Profile<br>Consolidate Addendums |
| 2.2 | 16.10.2012 | Projekt Team | Anpassungen für Mozilla Root Programm |
| 2.3 | 25.06.2013 | Kerstin Wagner | Anpassung des Intervalls der CRL Generierung |
| 2.4 | 02.07.2013 | Hans Augstburger | Ersatz von „Fixnet“ |
| 2.5 | 29.01.2014 | Patrick Graber | Ergänzung Zertifikatsprofil Saphir für All-in Signing Service, Typo Korrekturen |
| 2.6 | 02.09.2014 | Kerstin Wagner | Anpassungen in Kapitel 5, Auslagerung der Zertifikatsprofile in eigenständiges Dokument, Integration der Quarz EV Zertifikate, diverse Korrekturen und Updates |
| 2.7 | 02.10.2014 | Patrick Graber | Ergänzung Rubin CA 3 |
| 2.8 | 27.10.2014 | Patrick Graber | Ergänzung All-in Signing Service |
| 2.9 | 23.12.2014 | Stéphane Vaucher;<br>Kerstin Wagner | Generelle Anpassungen aus Legal Sicht (hauptsächlich i.Z.m. einerseits All-in Signing Service und andererseits allgemeiner Verständlichkeit des Dokuments als Vertragsbestandteil) |
| 2.10 | 06.10.2015 | Kerstin Wagner | Review 2015 |
| 2.11 | 20.04.2016 | Kerstin Wagner | Review und Update 2016;<br>Auslagerung der Beschreibungen der CAs der 1. Generation (CA 1) und SuisseID in ein eigenständiges Dokument |
| 2.12 | 06.01.2017 | H-P Waldegger | Anpassungen an neue Identifikationsvorschriften gem. ZertES Ausgabe vom 18. März 2016;<br>Anpassung bei Algorithmus und Schlüssellänge bei Rubin CA 3 (Kap 6.1.5) |
| 2.13 | 12.09.2017 | H-P Waldegger | Übergangsbestimmungen zur Ablösung dieses Dokuments durch neue CP/CPS Version 3 auf Basis des revidierten ZertES [14].<br>Löschen der Referenzen auf EV SSL Zertifikate (Root EV und "Quarz"). |
| 2.13 | 10.10.2017 | Governance Board | Freigabe |

**Referenzierte Dokumente:**


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

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

[3] SR 943.032.1, TAV: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 6. Dezember 2004 (Stand am 1. August 2011)

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

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

[6] ETSI TS 102 023: Policy Requirements for time-stamping authorities

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

[8] Addendum zum CPS [vorliegendes Dokument]: Beschreibung Profile der Zertifikate, Sperrlisten und Online Statusabfragen der Swisscom Digital Certificate Services

[9] Rollenkonzept der Swisscom Digital Certificate Services

[10] All-in Signing Service, www.swisscom.com/Signing-service

[11] Mobile ID, www.swisscom.ch/Mobile-id

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

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

swisscom

## Inhaltsverzeichnis

# 1 Einleitung

Dieses Dokument beschreibt das Certification Practice Statement (nachfolgend CPS) und ist eine Aussage über die Zertifizierungsrichtlinien von Swisscom Digital Certificate Services, einer Dienstleistung der Swisscom (Schweiz) AG (nachfolgend Swisscom) zur Ausgabe von qualifizierten und fortgeschrittenen Zertifikaten im Sinne des schweizerischen Bundesgesetzes über die elektronische Signatur (ZertES [1]), den daraus abgeleiteten technischen und administrativen Ausführungsbestimmungen in der VZertES [2] und den TAV [3], sowie über die Ausgabe und Verwaltung von qualifizierten und fortgeschrittenen Zertifikaten gemäss den Vorgaben „Sicherheitsanforderungen für Vertrauenswürdige Systeme, die Serversignaturen unterstützen“ [12].

Diesem Dokument zugehörig sind die Zertifizierungsrichtlinien (Certificate Policies, CP) der jeweiligen Zertifikatsklassen.

Das Ziel der vorliegenden CPS besteht darin, die Abläufe für die Ausgabe, Administration und Anwendung von Swisscom Digital Certificate Services derart festzulegen, dass ein sicherer, zuverlässiger und den gesetzlichen Anforderungen entsprechender Betrieb der angebotenen Zertifizierungsdienstleistungen sowie der Anwendung der ausgegebenen Zertifikate gewährleistet ist.

Im Weiteren gibt die CPS Auskunft über die Praktiken der Swisscom Digital Certificate Services zur Ausgabe von Zertifikaten.

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

Die Bezeichnung „qualifiziert“ in Bezug auf elektronische Signaturen und Zertifikate bedeutet, dass ein Dienstanbieter die Vorgaben des Bundesgesetzes über die elektronische Signatur (ZertES [1]), der dazugehörigen Verordnung (VZertES [2]) und die technischen und administrativen Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur (TAV [3]) erfüllt. Die Einhaltung dieser Vorgaben wird durch eine von der Schweizerischen Akkreditierungsstelle (SAS) akkreditierte Anerkennungsstelle geprüft. Danach ist die anerkannte Anbieterin von Zertifizierungsdiensten (nachfolgend CSP) berechtigt, Zertifikate für die Erstellung und Überprüfung von „qualifizierten“ elektronischen Signaturen anzubieten. Daneben kann die qualifizierte Signatur auch für den Herkunftsnachweis (Authentizität) und zum Schutz vor Veränderungen (Integrität) eingesetzt werden.

Mit dem am 1.1.2005 in Kraft getretenen Bundesgesetz über die elektronische Signatur wurde Art. 14 Abs. $2^{bis}$ Obligationenrecht (OR, SR 220) eingeführt, der die qualifizierte elektronische Signatur der eigenhändigen Unterschrift gleichstellt, womit es möglich wird, Willenserklärungen (insbesondere für den Abschluss von Verträgen) auch in Bereichen, in welchen die Schriftform im Sinn von Art. 12 ff. OR vorgeschrieben ist, mit qualifizierter elektronischer Signatur abzugeben, soweit nicht abweichende gesetzliche oder vertragliche Form- oder Zustellungsvorschriften bestehen.

Jedes Zertifikat ist nur so vertrauenswürdig wie die Verfahren, nach denen es ausgestellt wird. Swisscom teilt dazu Zertifikate in „Zertifikatsklassen“ ein. Je höher die Zertifikatsklasse, desto umfangreichere Identifikationsprüfungen liegen der Ausstellung eines Zertifikates zugrunde. Die Zertifikate selbst enthalten als Information die Angabe über die Klasse des Zertifikats. Für die höchste Zertifikatsklasse, das qualifizierte Zertifikat, muss eine Person bei einer Registrierungsstelle

persönlich in Erscheinung treten und alle im Zertifikat vermerkten Daten mit einem amtlichen Ausweis und eventuell zusätzlichen Bescheinigungen belegen.

## 1.1 Überblick

Diese CPS wurde von Swisscom zu folgendem Zweck erstellt:

- Erfüllung der Anforderungen an einen Anbieter von qualifizierten Zertifikaten gemäss ZertES [1] und den zugehörigen Ausführungsbestimmungen, [2] und [3]
- Erfüllung der Anforderungen an einen Anbieter von fortgeschrittenen Zertifikaten gemäss ElDI-V [4];
- Beschreibung der Dienstleistungen, Rollen, Limitationen und Verpflichtungen bei der Verwendung von qualifizierten Zertifikaten der Swisscom;
- Sicherstellung der Interoperabilität bei der Benutzung von Zertifikaten der Swisscom.

Die Struktur dieser CPS orientiert sich an den Vorgaben des RFC 3647 [5].

## 1.2 Identifikation des Dokuments

Identifikation:

- Titel: Swisscom Digital Certificate Services – Certification Practice Statement
- Version: 2.13
- Object Identifier (OID) für diese CPS: 2.16.756.1.83.2.1
  Diese OID identifiziert nur das vorliegende Dokument

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

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

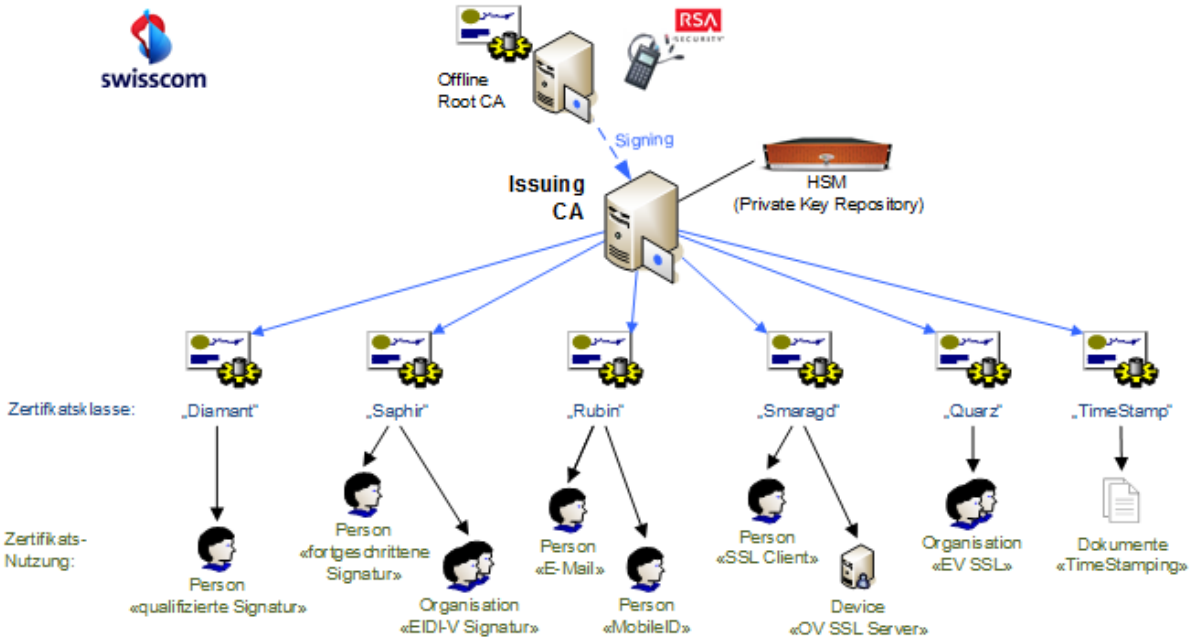
Die Stellen 6 bis 8 der OID von Swisscom Digital Certificate Services verweisen auf die jeweilige CA bzw. das jeweilige CP/CPS Dokument.

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

## 1.3 Beteiligte der Swisscom Digital Certificate Services

### 1.3.1 Certificate Authorities (CA)

Die Infrastruktur der Swisscom Digital Certificate Services ist hierarchisch aufgebaut:




Der Betrieb der hier aufgeführten Infrastruktur erfolgt ausschliesslich durch Swisscom.

#### 1.3.1.1 Root-CA

Der öffentliche Schlüssel (Public Key) der Root-CA ist in einem selbst signierten Zertifikat (Root-Zertifikat) abgelegt. Alle Teilnehmer der Swisscom Digital Certificate Services können das Zertifikat auf der Internet-Seite (http://www.swissdigicert.ch) beziehen und somit die Authentizität und Gültigkeit aller unterhalb dieses Wurzelzertifikates innerhalb der Swisscom Digital Certificate Services ausgestellten Zertifikate überprüfen.

Die Swisscom Root CA ist an keinem Netzwerk angeschlossen und wird nur dann gestartet, wenn sie benötigt wird. Die Root-CA stellt ausschliesslich Zertifikate für unmittelbar nachgelagerte Zertifizierungsstellen (CA) der Swisscom Digital Certificate Services aus.

Fingerprints der Root CA

| Name | Fingerprint Algorithmus | Fingerprint |
|---|---|---|
| Swisscom Root CA 2 | sha1 | 77 47 4f c6 30 e4 0f 4c 47 64 3f 84 ba b8 c6 95 4a 8a 41 ec |

Unterhalb der Root-CA werden folgende Certificate Authorities (CA) der Swisscom Digital Certificate Services betrieben:

#### 1.3.1.2 Diamant CA (qualifiziert)

Zur Ausgabe von Benutzer-Zertifikaten der Klasse Diamant. Entspricht den Anforderungen, welche das ZertES [1] für qualifizierte Zertifikate und qualifizierte elektronische Signaturen stellt. Der Zertifikatsinhaber verwendet eine sichere Signaturerstellungseinheit (SSCD). Der Schlüssel dient zur

Erstellung von qualifizierten elektronischen Signaturen im Sinn von Art. 2 Bst. e ZertES [1]. Dieser Typ von Zertifikaten wird nur für natürliche Personen ausgestellt, die allerdings juristische Personen vertreten können. Das Zertifikat kann ausschliesslich zum Signieren verwendet werden.

#### 1.3.1.3 Saphir-CA (fortgeschritten)

Zur Ausgabe von Benutzer- und Organisations-Zertifikaten der Klasse Saphir. Entspricht den Definitionen für digitale Zertifikate zur Erstellung von fortgeschrittenen Signaturen gemäss Art. 2 Bst. b ZertES [1] sowie den Anforderungen der ElDI-V [4] und verwendet eine sichere Signaturerstellungseinheit (SSCD). Dieser Typ von Zertifikaten wird für natürliche Personen und Organisationen ausgestellt und kann zum Signieren und Authentisieren verwendet werden.

#### 1.3.1.4 Rubin-CA

Zur Ausgabe von Zertifikaten der Klasse Rubin. Dies sind Soft-Zertifikate und setzen keine sichere Signaturerstellungseinheit (SSCD) voraus. Diese Klasse von Zertifikaten wird für interne Devices (z.B. Router, Access Points, etc.) Devices und Mobile ID ausgestellt und kann zum Signieren, Verschlüsseln und Authentisieren verwendet werden.

#### 1.3.1.5 Smaragd-CA

Zur Ausgabe von Zertifikaten der Klasse Smaragd. Dies sind Soft-Zertifikate und setzen keine sichere Signaturerstellungseinheit (SSCD) voraus. Diese Klasse von Zertifikaten wird für natürliche Personen, Organisationen und Devices ausgestellt und kann zum Signieren, Verschlüsseln und Authentisieren verwendet werden.

#### 1.3.1.6 Time-Stamping-CA

Zur Erstellung von Time-Stamping Signaturen. Entspricht den Anforderungen des VZertES [2] und des ETSI 102 023 [6] für qualifizierte Zertifikate. Jeder Time-Stamping Server hat ein eigenes Zertifikat. Der private Schlüssel für die Erstellung von Zeitstempel-Signaturen wird durch Swisscom in einem HSM erstellt.

### 1.3.2 Registrierungsstellen - Registration Authorities (RA)

Das Geschäftsmodell von Swisscom basiert auf einem Registration Authorities Vertragspartner-Modell. Dabei delegiert Swisscom ihre RA-Funktion an Vertragspartner (RA-Partner) und erlaubt diesen je nach Situation auch, Zertifikate selbst auszustellen. Je nach vertraglicher Vereinbarung steht es dem RA-Partner zu, Zertifikate nur innerhalb seiner Organisation abzugeben oder auch als „öffentliche“ RA aufzutreten.

Die RA-Partner werden mittels Vertrag verpflichtet, die von Swisscom definierten Prozesse für die Registrierung, Zertifikatsausgabe und Revokation einzuhalten. Sofern der RA-Partner auch qualifizierte Zertifikate ausgeben will, ist er in den Anerkennungsprozess durch eine durch die Schweizerische Akkreditierungsstelle (SAS) akkreditierte Anerkennungsstelle eingebunden. Gibt der RA-Partner nur fortgeschrittene Zertifikate aus, wird er durch Swisscom mindestens einmal jährlich überprüft.

Das Geschäftsmodell von Swisscom unterscheidet folgende Typen von RA:

- **Swisscom-RA**: Zur Ausgabe von Zertifikaten für den Eigengebrauch und für nachgelagerte Enterprise Registration Authorities.
- **Enterprise-RA** (nachfolgend E-RA): Ist ein RA-Partner, der in der Lage ist, innerhalb seiner Organisation Zertifikate direkt zu erstellen und auszugeben

- **Identity Validation Authority (nachfolgend Identitätsprüfstelle):** Ist ein RA-Partner, der als Registrierungsstelle Zertifikatsanträge entgegennimmt, die Angaben überprüft und einer zur Erstellung von Zertifikaten ermächtigten RA zur Ausführung weiterleitet.

Die Identitätsprüfung von Antragstellern wird von Mitarbeitern der Registrierungsstellen vorgenommen, bei qualifizierten Zertifikaten auf der Basis eines Vertrags, der die genauen Modalitäten der Delegation der RA-Tätigkeit nach Art. 9 Abs. 6 ZertES [1] regelt.

### 1.3.3 Zertifikatsinhaber (Subscriber)

Zertifikatsinhaber verwenden ihr Zertifikat, um Transaktionen, Dokumente und Kommunikation (z.B. E-Mail) elektronisch zu signieren oder zu verschlüsseln oder sich gegenüber einem Server oder einer Applikation zu authentisieren.

Vor der Überprüfung der Identität und Ausstellung eines Zertifikats ist ein Zertifikatsinhaber ein Antragsteller.

Die Vergaberegelungen für Zertifikate hängen von der Zertifikatklasse ab und werden in der zugehörigen CP, jeweils im Kapitel 3, beschrieben.

### 1.3.4 Zertifikatprüfer (Relying Parties)

Relying Parties sind Personen oder Unternehmen, die im Vertrauen auf ein Zertifikat, das von einem CSP ausgestellt wurde, handeln. Aussagen zur Zertifikatprüfung sind der zugehörigen CP zu entnehmen.

### 1.3.5 Weitere Teilnehmer

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

## 1.4 Anwendbarkeit der Zertifikate (Certificate Usage)

Der genaue Anwendungsbereich der Zertifikate wird in der zugehörigen CP, jeweils im Kapitel 1.4, beschrieben.

## 1.5 Verwaltung der Richtlinien

### 1.5.1 Organisation und Kontaktadresse

Die Verwaltung der Richtlinien (im Sinne der Definition und inhaltlichen Pflege) erfolgt im Auftrag des Governance Boards (siehe Kapitel 1.5.2) durch

Swisscom (Schweiz) AG
Digital Certificate Services
Postfach
8021 Zürich

Der Informatik Sicherheitsverantwortliche (ISO) erstellt in Zusammenarbeit mit Operations den CPS-Entwurf für den Swisscom-internen Vernehmlassungsprozess.

### 1.5.2 Verantwortung für die CPS

Die Gesamtverantwortung und die Entscheidungsgewalt für Inhalt und Einhaltung der CPS liegen innerhalb der Swisscom Digital Certificate Services beim Governance Board. Der Service Manager trägt gegenüber dem Governance Board die Verantwortung für die ordnungsmässige Erbringung der Dienstleistungen gemäss der verabschiedeten CPS.

Das Security Board analysiert Verstösse gegen die CPS und rapportiert an das Governance Board und den Service Manager.

## 1.6 Schlüsselwörter und Begriffe

| Begriff | Erklärung |
|---|---|
| Zertifizierungsstelle (CSP) | Eine Organisation, die digitale Zertifikate herausgibt und überprüft. |
| Anerkennungsstelle | Stelle, die nach dem Akkreditierungsrecht für die Anerkennung und die Überwachung der Anbieterinnen von Zertifizierungsdiensten akkreditiert ist. Die Anerkennungsstelle wird in der Schweiz von Schweizerischen Akkreditierungsstelle (SAS), ein Bereich des Staatssekretariats für Wirtschaft (SECO), akkreditiert. |
| Angaben zum Zertifizierungsbetrieb (CPS) | Angaben zu den Regeln und Richtlinien, die von der CSP für die Ausstellung von Zertifikaten effektiv umgesetzt werden. Die CPS definiert die Ausrüstungen, die Methoden und die Verfahren, die von der CSP in Übereinstimmung mit den von ihr gewählten Zertifikatsrichtlinien verwendet werden. |
| Benutzer/-in des Zertifikats (Relying Party) | Person oder Prozess, die oder der sich bei der Verwendung dieses Zertifikats auf die überprüften elektronischen Signaturen verlässt. |
| Certificate Authority (CA), Issuing CA | Instanz, die digitale Zertifikate ausstellt; in diesem Dokument wird damit das System bezeichnet, das Zertifikate ausstellt und signiert; es ist das zentrale Element einer PKI Infrastruktur |
| Digitales Zertifikat | elektronische Bescheinigung, die einen Signaturprüfschlüssel (private key) mit dem Namen einer Person, einer Organisation oder eines Systems verknüpft. |
| Elektronische Signatur, digitale Unterschrift | Technisches Verfahren zur Überprüfung der Echtheit eines Dokuments, einer elektronischen Nachricht oder der Identität des Absenders. Die elektronische Signatur und die handschriftliche Unterschrift werden bei Verwendung von digitalen Zertifikaten im Rahmen von Art. 14 Abs. 2bis OR als gleichwertig betrachtet. |
| Generierung der Zertifikate | Dienst der CSP; Erzeugung eines digitalen Zertifikats auf der Grundlage des Namens der Antragstellerin oder des Antragstellers eines Zertifikats und ihrer/seiner allfälligen Attribute, die bei der Registrierung überprüft werden. |
| Hash | Die Hashfunktion ist eine kryptografische Prüfsumme für einen Text, um deren Integrität sicher zu stellen. Das Verfahren dient der Reduzierung des Rechenaufwandes bei der Verschlüsselung von Daten im Public-Key-Verfahren. Auf die Nachricht, die eine variable Länge hat, wird eine Hashfunktion angewendet, die eine Prüfsumme fester Länge erzeugt, den Hashwert. Damit lässt sich die Integrität einer Nachricht zweifelsfrei feststellen. |
| Inhaber/-in des Zertifikats (Subscriber) | Natürliche Person, die Inhaberin des Signaturschlüssels ist, der dem im Zertifikat aufgeführten Signaturprüfschlüssel zugeordnet ist. |
| Liste der für ungültig erklärten Zertifikate (CRL) | von der CA signierte Liste, die die Seriennummern aller Zertifikate enthält, welche vor Ablauf ihrer Gültigkeit für ungültig erklärt wurden. |
| „On Demand“ Erzeugung und Nutzung von Schlüsselmaterial | „On Demand“ Erzeugung und Nutzung von Schlüsselmaterial (private und öffentliche Schlüssel sowie Zertifikate), die für die elektronische Signatur verwendet werden. Die Schlüsselpaare werden in der sicheren Umgebung der Zertifizierungsstelle erzeugt und verwendet. Unmittelbar nach der Signaturerzeugung wird der private Schlüssel gelöscht. |

| Begriff | Erklärung |
|---|---|
| Qualifizierte elektronische Signatur | elektronische Signatur, die folgende Anforderungen erfüllt (Art. 2 Bst. b, c und e ZertES [1]):<br>1. Sie ist ausschliesslich der Inhaberin oder dem Inhaber zugeordnet;<br>2. Sie ermöglicht die Identifizierung der Inhaberin oder des Inhabers;<br>3. Sie wird mit Mitteln erzeugt, welche die Inhaberin oder der Inhaber unter ihrer/seiner alleinigen Kontrolle halten kann<br>4. Sie wird durch eine sichere Signaturerstellungseinheit erzeugt;<br>5. Sie ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann<br>6. Sie beruht auf einem qualifizierten und zum Zeitpunkt der Erzeugung gültigen Zertifikat. |
| Qualifiziertes Zertifikat | digitales Zertifikat, das die Anforderungen von Art. 8 ZertES [1] erfüllt. |
| RDN-Namen, Relative Distinguished Name | Namen der Verzeichniseinträge, deren Eindeutigkeit sich auf einen bestimmten Eintrag bezieht und die Bestandteil eines Verzeichnisnamens (Distinguished Name) bilden. |
| Registrierung | Dienst der Registrierungsstelle, der darin besteht, die Identität und wenn nötig die Attribute jeder Antragstellerin und jedes Antragstellers eines Zertifikats zu überprüfen, bevor ihr/sein Zertifikat erzeugt oder die Aktivierungsdaten (oder das Passwort) zur Aktivierung der Nutzung des Signaturschlüssels zugewiesen werden. |
| Schlüsselpaar | Signaturschlüssel und dazugehörender Signaturprüfschlüssel, die mathematisch durch einen asymmetrischen Signaturalgorithmus miteinander verknüpft sind. |
| Sichere Signaturerstellungseinheit (SSCD) | Einheit nach Art. 6 Absatz 2 ZertES [1], die für die Implementierung des Signaturschlüssels konfiguriert ist, den die Inhaberin oder der Inhaber des Zertifikats zur Erstellung einer elektronischen Signatur verwendet. |
| Sicherheitspolitik (SP) | Gesamtheit von Regeln und Richtlinien, die auf Grund einer Risikoanalyse zur Reduzierung der Wahrscheinlichkeit von möglichen Zwischenfällen (vorbeugende Massnahmen) und zur Behebung der Auswirkungen solcher Zwischenfälle (Korrekturmassnahmen) ausgearbeitet wurden, um die für die Anbieterin von Diensten zur elektronischen Zertifizierung als schützenswert identifizierten Ressourcen zu schützen. Mit der Sicherheitsstrategie und -politik kann die gesamthaft zu erreichende Sicherheitsstufe für ein Informationssystem und besonders für jedes Element der Sicherheitsarchitektur eindeutig definiert werden. |
| Signaturprüfschlüssel (public key) | Daten wie Codes oder öffentliche kryptografische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden. |
| Signaturschlüssel (private key) | Einmalige Daten wie Codes oder private kryptografische Schlüssel, die von der Inhaberin oder vom Inhaber zur Erstellung einer elektronischen Signatur verwendet werden. |
| TrustCenter | Speziell geschützter Raum, in dem die Systeme der Zertifizierungsstelle betrieben werden. |
| Ungültigerklärung des Zertifikats | Dienst der Zertifizierungsstelle, der die Gültigkeit eines Zertifikats vor dessen Ablauf aufhebt. |
| Verteilung der Zertifikate | Dienst der Zertifizierungsstelle, der darin besteht, das Zertifikat nach seiner Generierung der Inhaberin oder dem Inhaber und - bei Einwilligung der Inhaberin oder des Inhabers - den Benutzerinnen und Benutzern des Zertifikats zur Verfügung zu stellen. |
| Verwaltung des Zertifikatstatus | Dienst der Zertifizierungsstelle, anhand dessen die Benutzerinnen und Benutzer eines Zertifikats überprüfen können, ob dieses für ungültig erklärt worden ist. |

| Begriff | Erklärung |
|---|---|
| Zeitstempel | Dienst der Zertifizierungsstelle, der eine mit dem Datum, der Uhrzeit und einer qualifizierten Signatur versehene Bescheinigung abgibt, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt existiert haben. |
| Zertifikatsrichtlinien (CP) | Gesamtheit von Regeln, welche die Anwendbarkeit eines Zertifikats für einen bestimmten Personenkreis und/oder eine Klasse spezieller Anwendungen mit gemeinsamen Sicherheitsanforderungen vorschreiben. |
| Zeitstempel-Objekt Empfänger (Relying Party) | Empfänger eines Zeitstempel-Objektes, der diesem Zeitstempel-Objekt vertraut |
| Zeitstempel-Dienst Benutzer (Subscriber) | Natürliche Person, die eigene oder Daten einer juristischen Person oder Organisation durch einen Zeitstempel-Dienst zeitstempelt. |
| Zeitstempel-Objekt, Time-stamp token | Datenobjekt, welches die Darstellung einer Tatsache mit einem bestimmten Zeitpunkt verknüpft und so den Beweis liefert, dass die Tatsache vor dem Zeitpunkt existiert hat. |
| Zeitstempel Policy, Time-stamp policy | Spezifikation genereller Prozesse, die vom Zeitstempeldienst während des Erstellens von signierten Zeitstempel-Objekten (Zeitstempel-Signaturen) verwendet werden. |
| Zeitstempel-Dienststelle, Time-Stamping Authority (TSA) | Dienststelle, die Zeitstempel-Objekte erstellt. |
| TSA Disclosure Statement | Aussagen über Methoden und Verfahren einer Zeitstempeldienststelle, die besonderen Nachdruck oder Bekanntmachung erfordert gegenüber dem Zeitstempel-Objekt Empfänger oder dem Zeitstempel-Dienst Benutzer, um z.B. regulative Anforderungen zu erfüllen. |
| TSA Practice Statement | Angaben zu den Regeln und Richtlinien, die von der Zeitstempeldienststelle für die Ausstellung von Zeitstempel-Signaturen effektiv umgesetzt werden. Die CPS definiert die Ausrüstungen, die Methoden und die Verfahren, die von der Zeitstempel-Dienststelle zur Ausgabe von Zeitstempel-Signaturen gemäss ZertES [1] angewendet werden. |
| Time-stamping unit | Die IT Infrastruktur, mit der Zeitstempel-Signaturen erstellt werden können. Auf dieser Infrastruktur existiert nur ein privater Schlüssel zur Ausstellung von Zeitstempel-Signaturen. |
| Coordinated Universal Time (UTC) | Universale Zeitskala auf Sekunden basierend. UTC ist definiert in der ITU-R Empfehlung TF.460-5 |
| Nonce | In der Kryptographie ist eine Nonce (Abkürzung für „a number used once“) eine Zahl, die nur einmal benutzt wird. Meist handelt es sich um eine Zufallszahl oder Pseudozufallszahl. Diese wird benutzt, um Reply-Attacken zu verhindern. |

## 1.7 Abkürzungen

| | |
|---|---|
| AIS | All-in Signing Service |
| BCP | Business Continuity Plan |
| CA | Certificate Authority |
| CERT | Computer Emergency Response Team; Team, das sicherheitskritische Themen erörtert, diskutiert und aktuelle Warnungen ausgibt |
| CN | Common Name, als Teil des DN |
| CP | Certificate Policy |
| CPS | Certification Practice Statement, Aussage über die Zertifizierungspraxen |
| CSP | Certificate Service Provider |
| CRL | Certificate Revocation List |
| DN | Distinguished Name gemäss RFC 3739 |
| EFD | Eidgenössisches Finanzdepartement |
| ETSI | European Telecommunications Standards Institute |
| ElDI-V | Verordnung des EFD über elektronisch übermittelte Daten und Informationen |
| HSM | Hardware Security Module |
| ISO | Information Security Officer, IT Sicherheitsverantwortlicher |
| LDAP | Lightweight Directory Access Protocol, Verzeichnisdienst |
| OCSP | Online Certificate Status Protocol, Dienst zur Online-Validierung von Zertifikaten |
| OID | Object Identifier |
| PED | PIN Entry Device |
| PIN | Personal Identification Number, Persönliche Nummer zum Aktivieren des Signaturschlüssels |
| PKI | Public Key Infrastruktur, Plattform zum Ausstellen, Verteilen und Prüfen digitaler Zertifikate |
| RA | Registration Authority, Registrierungsstelle (Umfasst Swisscom RA, E-RA und Identitätsprüfstelle) |
| RDN | Relative Distinguished Name |
| Re-Key | Zertifikaterneuerung mit neuen Schlüsseln |
| SSCD | Sichere Signaturerstellungseinheit, Secure Signature Creation Device |
| SSL | Secure Socket Layer, Sicherheitsprotokoll |
| TSP | Time Stamping Profile |
| IVA | Identity Validation Authority, Identitätsprüfstelle |
| TSA | Time-stamping Authority |
| TAV | Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate |
| VZertES | Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate |
| ZertES | Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate |

# 2 Veröffentlichungen und Verzeichnisdienst

## 2.1 Verzeichnisdienst

Swisscom stellt ihre Root-Zertifikate, Sperrlisten (CRL), CPs, CPS und Nutzungsbestimmungen im Web zur Verfügung.

Das Repository der Dienstleistungen von Swisscom Digital Certificate Services befindet sich auf:

http://www.swissdigicert.ch

Die Online-Dienste zur Abfrage der Root-Zertifikate, Sperrlisten und OCSP-Responses sind rund um die Uhr mit einer Verfügbarkeit von 99.9% zugänglich.

## 2.2 Veröffentlichung von Informationen

Swisscom Digitale Certificate Services publiziert die folgenden Informationen über http://www.swissdigicert.ch:

- Zertifikate der Root-und Issuing CAs der Swisscom: http://www.swissdigicert.ch/download_ca
- CPS und CP Dokumente: http://www.swissdigicert.ch/download_docs
- CRLs: http://www.swissdigicert.ch/download_crl
- Nutzungsbestimmungen: http://www.swissdigicert.ch/download_cond
- Status Meldungen
- Kontakt Angaben

## 2.3 Aktualisierung der Informationen

Neu ausgestellte Zertifikate, CRLs, Richtlinien und ggf. weitere Informationen werden zeitnah zur Verfügung gestellt. Es gelten die folgenden Veröffentlichungsfrequenzen:

- Zertifikate werden umgehend nach der Ausstellung veröffentlicht (falls dies für das betroffene Zertifikat in Frage kommt und vom Zertifikatsinhaber gewünscht wird)
- Sperrlisten (CRL): alle 2 Stunden
- Einträge in der CRL werden nicht gelöscht, die Listen werden lediglich ergänzt.
- Richtlinien (CP / CPS): nach Bedarf und nach Änderungen
- Weitere Informationen: nach Bedarf

## 2.4 Zugang zu den Informationsdiensten

Der lesende Zugriff auf die öffentlichen Informationen gemäss Kapitel 2.1. und 2.2 unterliegt keiner Zugangskontrolle.

Zertifikate sind öffentlich und können von allen Benutzern abgefragt werden, sofern die Zertifikate für die Publikation geeignet sind und vom Zertifikatsinhaber freigegeben wurden.

Im LDAP Verzeichnis werden keine vollen Wildcard Abfragen unterstützt.

# 3 Identifizierung und Authentisierung

## 3.1 Namen

### 3.1.1 Namensform

Alle innerhalb der Swisscom Digital Certificate Services ausgestellten Zertifikate beinhalten eindeutige Namen (distinguishedName, nachfolgend DN) entsprechend der Normenserie X.500.

Der DN jedes Zertifikats besteht aus folgenden Attributen:

- CN = Titel (optional), Vorname, Mittelname (optional), Name
  *oder* Name der Organisation
  *oder* Systemname
  *oder* Pseudonym;
- C = Ländercode des Landes, in dem der Antragsstellen den Wohnsitz hat, das vorgelegte Identifikations-Dokument des Zertifikatsinhabers ausgestellt wurde (natürliche Person) oder die Organisation ihren Sitz hat (juristische Person) gemäss ISO-Ländercode DIN EN ISO 3166-1);
- falls erforderlich (z.B. bei Namensgleichheit): Laufnummer = zusätzliche Nummer, die die Eindeutigkeit des DN sicherstellt.

Über diese Elemente lässt sich jedes Zertifikat eindeutig mit einem leserlichen Hinweis auf den Zertifikatsinhaber bzw. das System identifizieren. Die Zuordnung eindeutiger Zertifikats Seriennummern ist dem Addendum zu dieser CPS [8], Kapitel 2, zu entnehmen.

Weitere Attribute des DN sind möglich. Obligatorische und optionale Attribute, die in den DN aufgenommen werden müssen bzw. können, sind in der jeweiligen CP, Kapitel 3.1.1, detailliert beschrieben. Diese Beschreibungen beinhalten auch eine Präzisierung der Semantik und der Prüfungsanweisungen.

### 3.1.2 Aussagekraft von Namen

Der Name muss den Zertifikatsinhaber eindeutig identifizieren und in einer für Menschen verständliche Formen im „commonName“ (CN) des Zertifikates vorliegen. Bei der Namensvergabe gelten zusätzlich die folgenden Konventionen:

- *Natürliche Personen*
  Namenszusätze können nur verwendet werden, wenn diese in einem amtlichen Ausweispapier mit Lichtbild enthalten sind, z.B. „cn=Dr. Hans Peter Mustermann“.
- *juristische Personen und Organisationen*:
  - *qualifiziert*: Juristische Personen oder Organisationen können nur durch eine natürliche Person vertreten werden. Dazu wird ein Zertifikat an eine natürliche Person ausgegeben, wobei in den Feldern CN=, O= und OU= die entsprechenden Namen gemäss vorgelegtem amtlichen Dokument (z.B. Handelsregisterauszug) eingetragen werden. Wenn die natürliche Person, die den Signaturschlüssel kontrolliert, nicht im Zertifikat enthalten sein soll, ist der Firmenname als Pseudonym zu verwenden.
  - *fortgeschritten*: Fortgeschrittene Zertifikate für juristische Personen und Organisationen benötigen für die administrative Abwicklung eine natürliche Person. Im Zertifikat muss diese allerdings nicht vermerkt sein. Das Feld CN enthält den Namen der Organisation gemäss den vorgelegten amtlichen Dokumenten.

- *Pseudonyme*
  Können entweder in das gleichnamige dafür vorgesehene X.500 Namenselement aufgenommen oder der CN eines Pseudonyms beginnt mit dem Kennzeichen „PN:“, z.B. „cn=PN:Firmenzertifikat“.
- *Datenverarbeitungssysteme*
  Der CN eines Datenverarbeitungssystems sollte grundsätzlich den voll qualifizierten Domain-Namen, z.B. „cn=www.swissdigicert.ch“, enthalten.

### 3.1.3 Pseudonymität / Anonymität

Es gelten die Regelungen aus Kapitel 3.1.2. Die Swisscom und die RA-Partner bieten in begründeten Ausnahmen Pseudonym-Zertifikate an.

### 3.1.4 Regeln zur Interpretation verschiedener Namensformen

Die Zeichenkodierung ist UTF8-String für Text und IA5-String für E-Mail Adressen.

### 3.1.5 Eindeutigkeit von Namen

Die Vorgaben zur Eindeutigkeit von Namen sind der zugehörigen CP, jeweils Kapitel 3.1.5, zu entnehmen.

### 3.1.6 Identifizierung, Authentisierung und Markenschutz

Die Registrierungsstelle ist nicht verpflichtet, den DN auf Konformität mit Rechten Dritter zu überprüfen. Allein der Zertifikatinhaber ist für solche Überprüfungen verantwortlich. Falls die Registrierungsstelle über eine Verletzung solcher Rechte informiert wird, wird das Zertifikat ungültig erklärt.

## 3.2 Identitätsüberprüfung bei Neuantrag

### 3.2.1 Verfahren zur Überprüfung des Besitzes des privaten Schlüssels

Für qualifizierte Zertifikate werden die Signaturschlüssel im SSCD erzeugt und bei Bedarf für die Personalisierung auf sicherem Weg an eine RA verteilt. Beim Einsatz von HSM ist sicherzustellen, dass das Schlüsselpaar im HSM erzeugt wurde und das HSM so konfiguriert ist, dass der private Schlüssel nicht exportiert werden kann. Für qualifizierte Zertifikate ist somit kein Verfahren zur Überprüfung des Besitzes des privaten Schlüssels nötig.

Für fortgeschrittene Zertifikate mit SSCD (Zertifikatsklasse „Saphir“) werden die Schlüssel ebenfalls im SSCD erzeugt. Auch für diese Variante ist kein Verfahren zur Überprüfung des Besitzes des privaten Schlüssels nötig.

Alle anderen Zertifikatsanfragen sind als signierte Anträge an die Registrierungsstelle zu stellen.

### 3.2.2 Authentisierung einer natürlichen Person

Die Verfahren für die Identitätsprüfung einer natürlichen Person sind der CP der betroffenen Zertifikatsklasse zu entnehmen.

Die höchsten Anforderungen an die Identitätsprüfung gelten für die Zertifikatsklasse „Diamant“ (qualifizierte Zertifikate) und basieren auf Art. 9 ZertES [1] und Art. 5 VZertES [2].

### 3.2.3 Authentisierung einer juristischen Person oder sonstigen Organisation

Die Verfahren für die Identitätsprüfung einer juristischen Person (Verein, Stiftung, Aktiengesellschaft, Kommanditaktiengesellschaft, Gesellschaft mit beschränkter Haftung, Genossenschaft) oder sonstigen Organisation des Privatrechts (insbesondere Einzelfirma, Kollektivgesellschaft, Kommanditgesellschaft) sind der CP der betroffenen Zertifikatsklasse zu entnehmen.

Zertifikatsinhaber eines Zertifikats der Klasse „Diamant“ (qualifizierte Zertifikate) kann nur eine natürliche Person sein. Ein Antrag einer juristischen Person oder sonstigen Organisation für die Ausstellung qualifizierter Zertifikate ist deshalb abzulehnen. Die Authentisierung einer juristischen Person oder sonstigen Organisation für Zertifikate der Klasse „Diamant“ ist folglich ausgeschlossen.

### 3.2.4 Authentisierung einer öffentlich-rechtlichen Stelle

Die Verfahren für die Identitätsprüfung einer öffentlich-rechtlichen Stelle (Behörde, Gericht, Amt, Direktion, öffentlich-rechtliche Anstalt usw.) sind der CP der betroffenen Zertifikatsklasse zu entnehmen.

Zertifikatsinhaber eines Zertifikats der Klasse „Diamant“ (qualifizierte Zertifikate) kann nur eine natürliche Person sein. Ein Antrag einer öffentlich-rechtlichen Stelle für die Ausstellung qualifizierter Zertifikate ist deshalb abzulehnen. Die Authentisierung einer juristischen Person oder sonstigen Organisation für Zertifikate der Klasse „Diamant“ ist folglich ausgeschlossen.

### 3.2.5 Antragsteller mit hohem Risiko

Swisscom berücksichtigt Zwangsmassnamen, welche von der Schweizerischen Eidgenossenschaft erlassen werden, um Sanktionen durchzusetzen. Insbesondere werden

- Zertifikatsanträge für natürliche und juristische Personen, Gruppen und Organisationen, die auf der vom SECO publizierten Blacklist [1] bzw. auf der Blacklist der Organisation der Vereinten Nationen (UNO) [2] aufgeführt sind,
- sowie auch Zertifikatsanträge von Personen, welche die Aufnahme eines Attributs beantragen, welche die erwähnten Blacklists betreffen,

ohne Angabe von Gründen abgelehnt.

## 3.3 Identifizierung und Authentisierung bei einer Zertifikaterneuerung

### 3.3.1 Routinemässige Zertifikaterneuerung (re-key)

Diese Regelung ist in der zugehörigen CP, Kapitel 3.3.1, festgelegt.

### 3.3.2 Zertifikaterneuerung (re-key) nach einer Ungültigerklärung

Diese Regelung ist in der zugehörigen CP, Kapitel 3.3.2, festgelegt.

## 3.4 Identifizierung und Authentisierung bei einer Ungültigerklärung

Für die Ungültigerklärung eines Zertifikates ist grundsätzlich die Registrierungsstelle zuständig, bei der das Zertifikat beantragt wurde. Ein Widerruf kann auf folgende Arten erfolgen:

[1] https://www.seco.admin.ch/sanktionen-al-qaida-taliban
[2] https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

- Persönliche Vorsprache bei der Registrierungsstelle mit Angabe der Autorisierungsinformation bzw. Identitätsprüfung nach Kapitel 3.2.
- Telefon-Anruf bei der zuständigen Registrierungsstelle mit Angabe der Autorisierungsinformation.
- Übersendung eines unterzeichneten Widerrufsantrags unter Angabe der Seriennummer des Zertifikates per Post. Zur Verifikation der Identität wird der Zertifikatsinhaber zurückgerufen.
- Ausserhalb der Geschäftszeiten der zuständigen Registrierungsstelle kann die Swisscom Hotline unter der Nummer 0800 724 724 kontaktiert werden, die dann die Ungültigerklärung initialisiert. Zur Verifikation der Identität wird der Zertifikatsinhaber zurückgerufen.

# 4 Betriebsanforderungen für den Zertifikats Lebenszyklus

## 4.1 Zertifikatantrag

### 4.1.1 Wer kann ein Zertifikat beantragen

Diese Regelung ist in der zugehörigen CP, Kapitel 4.1.1, festgelegt.

### 4.1.2 Registrierungsprozess

Der Registrierungsprozess ist in der zugehörigen CP, Kapitel 4.1.2, beschrieben.

### 4.1.3 SSCD Verteilprozess

Die Registrierungsstelle erfasst und überprüft die Daten des Antragsstellers. Anschliessend archiviert sie die Daten im zentralen System der Swisscom, generiert das persönliche Schlüsselpaar des Antragstellers auf der vor-initialisierten SSCD und schützt das SSCD abschliessend mit einer PIN. Anschliessend werden das SSCD und der PIN-Brief auf separaten Wegen über eingeschriebene Briefpost an den Zertifikatsinhaber geschickt.

Nach dem Empfang der SmartCard sollte der Karteninhaber umgehend den PIN Code ändern.

## 4.2 Bearbeitung von Zertifikatanträgen

Diese Regelungen sind in der zugehörigen CP, Kapitel 4.2, beschrieben.

## 4.3 Zertifikatausstellung

Die Zertifikate der Klassen „Diamant“ und „Saphir“ werden ausschliesslich auf von Swisscom gemäss TAV [3] homologierten SSCD ausgestellt. Dabei wird die Generierung des Schlüsselpaars in der sicheren Umgebung der Swisscom durchgeführt.

Für qualifizierte Zertifikate („Diamant“) und fortgeschrittene Zertifikate der Klasse „Saphir“ kommen nur SSCD zum Einsatz, die eine der gemäss Abs. 2.2.3 TAV [3] geforderten Zertifizierungen erfolgreich durchlaufen haben und die mindestens FIPS 140-2 Level 3 zertifiziert sind.

Weitere Details sind den zugehörigen CPs, jeweils Kapitel 4.3, zu entnehmen.

## 4.4 Zertifikat-Akzeptanz

Der Zertifikatinhaber ist verpflichtet, die Korrektheit der Einträge auf dem eigenen Zertifikat (beispielsweise DN) sowie der Zertifikatskette nach Erhalt zu verifizieren. Dazu kann z.B. die Zertifikats-Anzeige eines Internet Browsers oder ein PDF Reader benutzt werden.

### 4.4.1 Annahme des Zertifikats

Ein Zertifikat wird durch den Zertifikatsinhaber akzeptiert und dadurch gültig, wenn

- das Zertifikat verwendet wird oder
- der Zertifikatsinhaber ausdrücklich die Annahme erklärt oder
- innerhalb von 10 Tagen nach Erhalt kein Widerspruch erfolgt.

Fehlerhaft ausgestellte Zertifikate hat die ausstellende RA unverzüglich für ungültig zu erklären.

### 4.4.2 Veröffentlichung des Zertifikats

Ein von Swisscom ausgestelltes Zertifikat wird nach der Ausstellung unverzüglich über den Verzeichnisdienst veröffentlicht, sofern der Zertifikatbesitzer dazu sein Einverständnis gibt und sich das Zertifikat überhaupt für die Veröffentlichung eignet (was bei Zertifikaten mit einer Gültigkeitsdauer, die kürzer ist als das Aktualisierungs-Intervall der CRL (wie z.B. bei AIS OnDemand) nicht der Fall ist).

### 4.4.3 Benachrichtigung weiterer Instanzen

Eine Benachrichtigung weiterer Instanzen ist nicht vorgesehen.

## 4.5 Verwendung des Schlüsselpaares und des Zertifikats

Diese Regelungen sind in der zugehörigen CP, Kapitel 4.5, festgelegt.

## 4.6 Zertifikaterneuerung (Certificate renewal)

Diese Regelungen sind in der zugehörigen CP, Kapitel 4.6, festgelegt.

## 4.7 Zertifikaterneuerung (Re-Key)

Diese Regelungen sind in der zugehörigen CP, Kapitel 4.7, festgelegt.

## 4.8 Zertifikatmodifizierung

Eine Modifizierung von Zertifikaten wird nicht angeboten.

Bei einer Änderung an einem im Zertifikat eingetragenen Attribut wird ein neues Zertifikat ausgestellt.

## 4.9 Ungültigerklärung und Suspendierung von Zertifikaten

Der Ablauf einer Identifizierung und Authentisierung bei einer Ungültigerklärung ist in Kapitel 3.4 beschrieben.

Der Prozess läuft folgendermassen ab:

- Der Zertifikatsinhaber oder die juristische Person, die der Zertifikatsbesitzer gemäss einem im Zertifikat vermerkten Attribut vertritt, richten den Antrag für die Ungültigerklärung an die zuständige Registrierungsstelle.
- Die Registrierungsstelle überprüft die Identität des Antragstellers und die Begründung für die Ungültigerklärung.
- Nach erfolgreicher Prüfung wird das entsprechende Zertifikat durch die Registrierungsstelle ungültig erklärt.
- Swisscom veröffentlicht die aktualisierte CRL mit den ungültig erklärten Zertifikaten.

Eine Suspendierung von Zertifikaten wird nicht angeboten.

Weitere Details sind den jeweiligen CPs, Kapitel 4.9, zu entnehmen.

## 4.10 Dienst zur Statusabfrage von Zertifikaten

Swisscom bietet mehrere Verfahren für die Statusabfrage von Zertifikaten an.

### 4.10.1 Verfahrensmerkmale

Über folgende Verfahren kann ein Zertifikatsnutzer die Gültigkeit eines Zertifikates prüfen

- Der Status eines Zertifikates kann über die Webseite der Swisscom Digital Certificate Services im Menü *Zertifikatsabfrage* online abgefragt werden (http://www.swissdigicert.ch/cert_query ). Dabei kann unter Eingabe eines im CN enthaltenen Feldes (Name, Vorname, Organisation, etc.) oder der Seriennummer der Status eines Zertifikates abgefragt werden.

  Diese Statusabfrage steht für Zertifikate, deren Lebensdauer kürzer ist als das Aktualisierungsintervall der CRL (siehe Kapitel 2.3), nicht zur Verfügung.
- Es wird ein OCSP-Dienst für die online Statusabfragen über das Internet angeboten.
- Über eine LDAP Abfrage kann mit den entsprechenden Parametern zur Identifikation des DN kann der Status eines Zertifikates abgefragt werden.
- Auf der Internetseite der Swisscom Digital Certificate Services können die aktuellen CRLs heruntergeladen werden (http://www.swissdigicert.ch/download_crl).
- Ein Internet Browser kann ebenfalls dazu genutzt werden, den Inhalt eines Zertifikats im Detail anzuzeigen.

### 4.10.2 Verfügbarkeit der Dienste

Die Online Zertifikat-Abfrage über den Web-Server, LDAP, die CRL sowie OCSP stehen rund um die Uhr zur Verfügung. Für die Validierungs-Dienste garantiert Swisscom eine Verfügbarkeit von 99.9%.

### 4.10.3 Optionale Merkmale

Die Verfügbarkeit der Services wird durch Swisscom permanent überwacht. Alle wichtigen Komponenten, die zur Bereitstellung der-Zertifikat-Abfrage über den Web-Server und über LDAP notwendig sind, als auch die Bereitstellung der CRLs und OCSP sind redundant ausgelegt und unterstützen eine automatische Umschaltung im Falle eines Problems.

### 4.11 Beendigung des Vertragsverhältnisses durch den Zertifikatsinhaber

Diese Regelungen sind in der zugehörigen CP, Kapitel 4.11, festgelegt.

### 4.12 Schlüsselhinterlegung und -wiederherstellung

Schlüsselhinterlegung und –Wiederherstellung (Key Escrow oder Key Recovery) ist für qualifizierte Signaturschlüssel der Zertifikatsklasse „Diamant“ gemäss ZertES [1] nicht erlaubt und wird nicht angeboten. Dasselbe gilt für die Zertifikatsklasse „Saphir“ aufgrund der regulatorischen Anforderungen von ElDI-.

## 5 Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen

Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen zum Betrieb der Swisscom Digital Certificate Services entsprechen den Vorgaben des ZertES [1], den TAV [3] sowie den anderen referenzierten Dokumenten.

Einzelne Richtlinien wie zum Beispiel das Rollenkonzept oder die Zutritts Policy können in eigenständigen Dokumenten vorliegen, die nicht zwingend veröffentlicht werden.

### 5.1 Infrastrukturelle Sicherheitsmassnahmen

#### 5.1.1 Lage und Konstruktion

Die technischen Systeme der Swisscom Digital Certificate Services inklusive der CA-Services befinden sich in speziell gesicherten Räumen der Swisscom (sog. TrustCenter). Die wichtigen Komponenten sind redundant ausgelegt und befinden sich in zwei getrennten Rechenzentren. Die Gebäude der beiden Rechenzentren sind ausreichend (mehr als 30 km) voneinander entfernt, so dass nicht beide vom selben Naturereignis oder Katastrophe betroffen werden können. Die Gebäude befinden sich in Bern und Zürich.

Die Räume bieten hinsichtlich der infrastrukturellen Sicherheitsmassnahmen einen ausreichenden Schutz und entsprechen den Vorgaben der TAV [3], sowie den anderen referenzierten Dokumenten.

#### 5.1.2 Zutrittskontrolle

Die Betriebsräume von SDCS sind durch geeignete technische und infrastrukturelle Massnahmen gesichert, so dass nur berechtigte Mitarbeiter Zutritt haben, die eine Rolle innerhalb der Betriebsorganisation wahrnehmen und autorisiert wurden. Der Zutritt durch betriebsfremde Personen wird durch eine Besucherregelung festgelegt. Der Zutritt zum TrustCenter ist durch eine Zutrittsanlage mit biometrischen Erkennungsverfahren geschützt.

#### 5.1.3 Stromversorgung und Klimatisierung

Die Rechenzentren der Swisscom verfügen über eine unterbruchsfreie Stromversorgung. Kurzzeitige Unterbrüche werden durch Akkus überbrückt. Bei längeren Stromausfällen liefert ein Diesel-Notstromaggregat die notwendige Energie. Die Notstromversorgung ist doppelt (redundant) ausgelegt.

#### 5.1.4 Abwehr von Wasserschäden

Die Räume für die technische Infrastruktur verfügen über einen angemessenen Schutz vor Wasserschäden.

### 5.1.5 Feuer

Die Rechnerräume verfügen über Brandmeldeanlagen wobei der Raum und der Hohlboden mit Rauchmeldern ausgestattet sind.

Die bestehenden Brandschutzvorschriften werden eingehalten, Handfeuerlöscher sind in ausreichender Anzahl vorhanden.

### 5.1.6 Datenträger

Datenträger werden in verschlossenen Räumen oder Schränken aufbewahrt. Datenträger mit sensiblen Daten werden in einem Tresor aufbewahrt, sofern sie sich nicht in einem Rechenzentrum der Swisscom befinden.

### 5.1.7 Abfallentsorgung

Informationen auf elektronischen Datenträgern werden sachgemäss vernichtet und anschliessend durch einen Dienstleister sachgerecht entsorgt. Papierdatenträger werden mittels vorhandenen Aktenvernichtern zerstört und durch einen Dienstleister sachgerecht entsorgt.

### 5.1.8 Externes Backup

Die kritischen Komponenten zur Sicherstellung eines unterbruchsfreien Betriebs sind auf zwei Rechenzentren aufgeteilt. Die Backups des Rechenzentrums 1 werden im Rechenzentrum 2 und umgekehrt aufbewahrt.

Die Backups der privaten Schlüssel der Root CAs sind angemessen geschützt in einem Bankschliessfach gelagert.

## 5.2 Organisatorische Sicherheitsmassnahmen

### 5.2.1 Vertrauenswürdige Rollen

Vertrauenswürdige Rollen müssen von Personen übernommen werden, die einer regelmässigen Überprüfung unterliegen. Solche Personen können Swisscom Mitarbeiter, Vertragspartner und Berater sein. Sie haben Zugriff auf die Systeme von Swisscom Digital Certificate Services und führen Identitätsüberprüfungen oder kryptographische Operationen aus, die wesentliche Auswirkungen haben können auf:

- Die Validierung von Informationen in Zertifikatsanträgen
- Die Annahme, Ablehnung oder sonstige Verarbeitung von Zertifikatsanträgen
- Sperranträge oder Enrollment Informationen
- Die Ausgabe oder den Widerruf von Zertifikaten
- die Handhabung der Informationen oder Anfragen der Zertifikats Besteller.

Vertrauenswürdige Personen umfassen, sind aber nicht beschränkt auf:

- Administratoren von kryptographischen Systemen
- System-Administratoren
- Engineers
- Information Security Officer
- Sicherheitspersonal
- zuständige Führungskräfte

Die Aufgaben und Pflichten von Personen in vertrauenswürdigen Rollen werden so verteilt, dass eine Person nicht allein handeln und so die Sicherheitsmassnahmen umgehen und die Vertrauenswürdigkeit der PKI oder TSA-Operationen untergraben kann. Die Zuweisung von vertrauenswürdigen Rollen an Personen wird jährlich überprüft.

Personen, die eine vertrauenswürdige Rolle anstreben, müssen die Anforderungen aus Kapitel 5.3 erfüllen.

### 5.2.2 Anzahl erforderlicher Mitarbeiter pro Aufgabe

Der Betrieb der Swisscom Digital Certificate Services erfordert, dass mindestens zwei in einer vertrauenswürdigen Rolle handelnde Personen zusammenarbeiten, um im Vier-Augen-Prinzip Operationen auf den kryptografischen Devices durchzuführen (private Schlüssel aktivieren, CA-Schlüsselpaar erzeugen, Sicherung der privaten Schlüssel erstellen etc.).

### 5.2.3 Identifizierung und Authentisierung der Rollen

Die Identifizierung und Authentisierung der Rollen erfolgt auf Grundlage des Rollenmodells von Swisscom Digital Certificate Services [9]. Der technische Zugang zu den einzelnen IT-Systemen wird durch starke Authentisierung (SSCD) oder Benutzerkennung und Passwort realisiert.

Kryptografische Devices wie HSM und CA-Server sind besonderen Authentisierungsverfahren unterworfen. Bei einem „Admin"-Zugriff auf diese Komponenten ist das Passwort zweigeteilt zwischen dem Security Device Administrator (SECADM) und dem Information Security Officer (ISO). Alle Zugriffe erfolgen im „4-Augen-Prinzip".

### 5.2.4 Trennung von Aufgaben

Ein Mitarbeiter kann innerhalb einer Gruppe in mehr als einer Rolle auftreten. Gruppenübergreifende Doppelbelegungen sind aufgrund von Anforderungen an die funktionale Trennung untersagt. Es ist möglich, dass Funktionen einer Rolle auf mehrere Mitarbeiter verteilt werden.

In der folgenden Tabelle ist aufgeführt, welche Rollen miteinander unverträglich sind (rot markiert).

| Incompatible with | Administration/Lead | Service Manager | Product Manager | Lead Engineer | Configuration and Ops | Head of Operations | Security Device Administrator | System Administrator | 1st Level Support | 2nd Level Support | 3rd Level Support | Security Manager on Duty | Change Manager | Building Sec. Organization | Perimeter Administrator | Perimeter Security Engineer | Local Security Officer | Controlling | Security Board | Governance Board | Change Advisory Board | Global RA | Information Sec. Officer | Internal Audit | System Auditor | Miscellaneous | Legal & Compliance | Human Resources |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Administration/Lead** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Service Manager | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Product Manager | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Lead Engineer | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Configuration and Ops** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Head of Operations | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Security Device Administrator | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System Administrator | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1st Level Support | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2nd Level Support | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3rd Level Support | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Security Manager on Duty | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Change Manager | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Building Sec. Organization | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Perimeter Administrator | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Perimeter Security Engineer | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Local Security Officer | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Controlling** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Security Board | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Governance Board | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Change Advisory Board | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Global RA | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Information Sec. Officer | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Internal Audit | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System Auditor | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Miscellaneous** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Legal & Compliance | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Human Resources | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

## 5.3 Personelle Sicherheitsmassnahmen

### 5.3.1 Anforderungen an die Mitarbeiter

Die Mitarbeiter von Swisscom, welche für den Betrieb der Plattform oder die Überwachung zuständig sind, erfüllen alle notwendigen Anforderungen hinsichtlich Vertrauenswürdigkeit, Integrität, Zuverlässigkeit und Fachkunde. Neben einer allgemeinen Ausbildung auf dem Gebiet Informationstechnik verfügen die Mitarbeiter in ihrer Rolle über angemessene Fachkenntnisse in den Bereichen:

- Sicherheitstechnologie, Kryptographie, elektronische Signaturen, PKI,
- Internationale Standards, technische Normen,
- Betriebssysteme, TCP/IP Netzwerke und LDAP.

### 5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Von allen Mitarbeitern der Swisscom Digital Certificate Services, Plattform Management & Operations liegt ein Strafregister- und ein Betreibungsregisterauszug vor, die alle drei Jahre erneut vorzulegen sind.

Betriebsfremde Personen dürfen nur in Begleitung von autorisierten Mitarbeitern der Swisscom die Betriebsräume betreten.

### 5.3.3 Anforderungen an die Schulung

In der Betriebsorganisation des Swisscom Digital Certificate Services werden ausschliesslich qualifizierte Mitarbeiter eingesetzt. Darüber hinaus werden regelmässige Schulungen für alle Mitarbeiter der Betriebsorganisation durch kompetente Personen durchgeführt.

Ein Mitarbeiter erhält erst nach Nachweis der notwendigen Fachkunde eine Berechtigung, eine spezifische Rolle auszuführen.

### 5.3.4 Frequenz von Schulungen

Die Frequenz der Schulungen orientiert sich an den Anforderungen. Schulungen werden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und Sicherheitstechnik durchgeführt.

### 5.3.5 Ablauf und Sequenz der Job Rotation

Der Ablauf und die Sequenz der Job Rotation richtet sich nach den Anforderungen der Swisscom oder eines bestimmten Mitarbeiters. Ein Arbeitsplatztausch ist nicht zwingend erforderlich.

### 5.3.6 Sanktionen für unautorisierte Handlungen

Unautorisierte Handlungen, die die Sicherheit der IT-Systeme der Swisscom Digital Certificate Services gefährden oder gegen Datenschutzbestimmungen verstossen, werden disziplinarisch geahndet. Bei strafrechtlicher Relevanz werden die zuständigen Behörden informiert.

### 5.3.7 Anforderungen an die Arbeitsverträge

Für die Arbeitsverträge der Mitarbeiter der Swisscom gilt das schweizerische Gesetz. Alle Mitarbeiter der Swisscom Digital Certificate Services haben eine Geheimhaltungserklärung unterzeichnet.

### 5.3.8 Dokumente für die Mitarbeiter

Den Mitarbeitern der Swisscom Digital Certificate Services stehen folgende Dokumente zur Verfügung:

- Zertifizierungsrichtlinien (CP)
- Erklärung zu den Zertifizierungspraktiken (CPS)
- Sicherheitskonzept
- Rollenbeschreibung
- Prozessbeschreibungen und Formulare für den regulären Betrieb
- Verfahrensanweisungen für den Notfall
- Dokumentation der IT-Systeme
- Bedienungsanleitungen für die eingesetzte Software

## 5.4 Sicherheitsüberwachung

### 5.4.1 Überwachte Ereignisse

Zur Abwehr von Angriffen und zur Kontrolle der ordnungsgemässen Funktion der Infrastruktur der Swisscom Digital Certificate Services werden die nachfolgenden Massnahmen ergriffen.

Folgende Klassen von Ereignissen werden in Form von Log-Dateien oder Papierprotokollen erfasst:

- Betrieb der IT-Komponenten, u.a.

- Bootvorgänge der Hardware
- Fehlgeschlagene Login-Versuche
- Vergabe und Entzug von Berechtigungen
- Installation und Konfiguration der Software

- Alle Transaktionen der Zertifizierungsstelle, u.a.
  - Zertifikatanträge
  - Zertifikatauslieferung
  - Zertifikatveröffentlichung
  - Zertifikatrevokation
  - Schlüsselerstellung
  - Zertifikaterstellung
- Änderungen der Richtlinien und des Betriebshandbuchs, u.a.
  - Rollendefinitionen
  - Prozessbeschreibungen
  - Wechsel der Verantwortlichkeiten
- Physische Sicherheit
  - Zutritte zu Datencenter
  - Technische Alarme
  - Einbruchmeldung

### 5.4.2 Frequenz der Protokollanalyse

Eine Überprüfung der Protokolldaten findet gemäss internen Richtlinien statt.

### 5.4.3 Aufbewahrungszeitraum für Protokolldaten

Sicherheitsrelevante Protokolldaten werden entsprechend den gesetzlichen Regelungen aufbewahrt. Die Aufbewahrungsdauer von Protokolldaten bezüglich des Schlüssel- und Zertifikatmanagements entspricht der Gültigkeitsdauer des Zertifikats der CA, zuzüglich 11 Jahren.

### 5.4.4 Schutz der Protokolldaten

Die Protokolldaten werden auf einen zentralen Log Server übertragen und so gegen Zugriff, Löschung und Manipulation geschützt und sind nur den System- bzw. Netzwerkadministratoren zugänglich.

### 5.4.5 Backup der Protokolldaten

Die Protokolldaten werden zusammen mit anderen relevanten Daten der Infrastruktur der Swisscom Digital Certificate Services einem regelmässigen Backup unterzogen.

### 5.4.6 Überwachungssysteme

Alle wesentlichen Komponenten des Services werden 7x24h pro-aktiv auf Verfügbarkeit überwacht. Die CAs und der Verzeichnisdienst werden mit geeigneten Verfahren überwacht und vor unautorisierten Änderungen geschützt.

### 5.4.7 Benachrichtigung bei schwerwiegenden Ereignissen

Über schwerwiegende Ereignisse werden unverzüglich der Sicherheitsverantwortliche für die Plattform (ISO) und nachfolgend das Security Board in Kenntnis gesetzt. In Zusammenarbeit mit den Systemadministratoren werden notwendige Aktionen festgelegt, um auf die Ereignisse adäquat reagieren zu können, ggf. wird die Geschäftsleitung informiert.

### 5.4.8 Schwachstellenuntersuchung

Eine Schwachstellenuntersuchung findet über automatisierte Tools im Perimeter (DMZ) und in den Netzwerksegmenten der Plattform statt. Die Resultate werden vom ISO regelmässig überprüft.

## 5.5 Archivierung

### 5.5.1 Archivierte Daten

Archiviert werden Daten, die für den Zertifizierungsprozess relevant sind:

- Alle von der CA ausgestellten Zertifikate
- Anträge auf Ungültigerklärung
- Widerrufslisten (CRL's)

Des Weiteren werden u.a. folgende intern benötigten Daten archiviert:

- CA-Root-Zertifikat und CA-Zertifikate für „Diamant“, „Saphir“, „Smaragd“, „Rubin“ und„Time-Stamping“ , inklusive der zugehörigen privaten Schlüssel;
- Verträge und Zertifikatanträge (inklusive dazugehörige Belege), diese enthalten persönliche Daten des Zertifikatsinhabers;
- Tätigkeitsjournal von Swisscom Digital Certificate Services.

Geräte und Applikationen werden solange vorgehalten, wie dies zur Erfüllung gesetzlicher und regulatorischer Anforderungen notwendig ist. Alternativ muss eine rechtzeitige Datenkonvertierung stattfinden.

### 5.5.2 Aufbewahrungszeitraum für archivierte Daten

Es gelten die Regelungen, die in Kapitel 5.4.3. beschrieben werden.

### 5.5.3 Schutz der Archive

Es wird durch geeignete Massnahmen sichergestellt, dass die Daten nicht verändert oder gelöscht werden können. Sind in den Archiven personenbezogene Daten enthalten, wird darüber hinaus sichergestellt, dass die Daten nicht unbefugt gelesen oder kopiert werden können.

### 5.5.4 Datensicherungskonzept

Die in den Kapiteln 5.4.1 und 5.5.1 aufgeführten Daten werden auf Grundlage eines Datensicherungskonzepts regelmässig einer Offline-Sicherung unterzogen.

Eckwerte des Datensicherungskonzepts:

- inkrementelles Backup an jedem Werktag
- wöchentliches vollständiges Backup
- monatliches Archivbackup

Die Backups werden jeweils überkreuz in den beiden Datenzentren aufbewahrt.

### 5.5.5 Anforderungen für Zeitstempel

Es gelten die Anforderungen gemäss Art. 13 VZertES [2] und Ziffer 2.4 TAV [3].

### 5.5.6 Archivierungssystem

Es wird ein internes Archivierungssystem verwendet.

### 5.5.7 Prozeduren zum Abrufen und Überprüfen von archivierten Daten

Der ISO kann den Abruf und die Prüfung der archivierten Daten autorisieren.

## 5.6 Schlüsselwechsel

Die Gültigkeitsdauer von Schlüsseln ist in Kapitel 6.3.2 festgelegt. Die Regelungen für einen Schlüsselwechsel bei Zertifikatsinhabern sind in der zugehörigen CP festgelegt. Falls einer der Schlüssel der Zertifizierungsstelle kompromittiert wurde, gelten die in Kapitel 5.7.3. aufgeführten Regelungen.

## 5.7 Kompromittierung und Wiederherstellung

### 5.7.1 Prozeduren bei Sicherheitsvorfällen und Kompromittierung

Die Prozeduren zur Behandlung von Sicherheitsvorfällen und bei der Kompromittierung von privaten Schlüsseln der Zertifizierungsstelle sind in einer Verfahrensanweisung für den Notfall dokumentiert. Diese Anweisung ist allen Mitarbeitern zugänglich.

Sicherheitsvorfälle können der entsprechenden Registrierungsstelle oder direkt dem Swisscom Call Center unter der Telefonnummer 0800 724 724 gemeldet werden.

### 5.7.2 Prozeduren bei IT-Systemen

Werden innerhalb der SDCS Plattform fehlerhafte oder manipulierte Rechner, Software und/oder Daten festgestellt, die Auswirkungen auf die Prozesse der Zertifizierungsstelle haben, wird der Betrieb des entsprechenden IT-Systems unverzüglich eingestellt. Das IT-System wird auf einer Ersatz-Hardware unter Wiederherstellung der Software und der Daten aus der Datensicherung neu aufgesetzt, überprüft und in einem sicheren Zustand in Betrieb genommen. Anschliessend wird das fehlerhafte oder modifizierte IT-System analysiert.

Bei Verdacht einer vorsätzlichen Handlung werden gegebenenfalls rechtliche Schritte eingeleitet. Darüber hinaus erfolgen eine Bewertung der Sicherheit und eine Revision zur Aufdeckung von Schwachstellen. Gegebenenfalls werden zusätzliche Abwehrmassnahmen zur Vermeidung ähnlicher Vorfälle ergriffen. Die Mitarbeiter der Zertifizierungsstelle arbeiten in diesen Fällen mit den Experten des Swisscom-CERTs zusammen. Falls sich in einem Zertifikat fehlerhafte Angaben befinden, wird der Zertifikatsinhaber unverzüglich informiert und das Zertifikat widerrufen.

### 5.7.3 Kompromittierung von privaten Schlüsseln einer CA

Wurde der private Schlüssel einer Issuing CA kompromittiert oder besteht ein begründeter Verdacht auf eine Kompromittierung, so wird umgehend das Security Board informiert. Dieser überprüft eine festgestellte Kompromittierung oder einen Verdacht und ordnet gegebenenfalls den Widerruf betroffener Zertifikate an.

In diesem Fall werden folgende Massnahmen ergriffen:

- Unverzügliche Information aller direkt betroffenen Zertifikatsinhaber;

- Widerruf des Zertifikats der Zertifizierungsstelle und aller Zertifikate, die mit dem Zertifikat zertifiziert wurden. Gegebenenfalls Abschaltung der Verzeichnisdienste und der Statusabfragen, um inkorrekte oder ungültige Aussagen durch die Dienste zu verhindern;
- Erzeugung eines neuen Schlüsselpaares und eines Zertifikats für die Zertifizierungsstelle;
- Veröffentlichung des Zertifikats der Zertifizierungsstelle;
- Ausstellung neuer Zertifikate für die Zertifikatsinhaber nach Vorgabe durch das Security Board.

### 5.7.4 Betrieb nach einer Katastrophe

Eine Wiederaufnahme des Zertifizierungsbetriebs nach einer Katastrophe bei Verlust ist Bestandteil der Notfallplanung und kann innerhalb kurzer Zeit erfolgen, sofern die Sicherheit der Zertifizierungsdienstleistung gegeben ist. Die Bewertung der Sicherheitslage obliegt dem Security Board.

## 5.8 Einstellung des Betriebs

Die Bedingungen an die Einstellung der Geschäftstätigkeiten sind in Art. 14 ZertES [1], Art. 12 VZertES [2] und Kapitel 7.4.9 ETSI TS 101 456 festgelegt.

Falls es zur Einstellung des Zertifizierungsbetriebs kommen sollte, werden gemäss den gesetzlichen Vorschriften folgende Massnahmen ergriffen:

- Benachrichtigung der Anerkennungsstelle und des SAS/SECO
- Benachrichtigung aller Zertifikatsinhaber, Registrierungsstellen und der betroffenen Organisationen, mindestens drei Monate vor Einstellung der Tätigkeit
- Benachrichtigung der Öffentlichkeit
- Widerruf aller noch gültigen Zertifikate bis zum Terminierungsstichtag
- Übergabe der endgültigen Certificate Revocation List (CRL), des Transaktionsjournals und zugehöriger Belege an die von SAS benannte Stelle
- Sichere Zerstörung der privaten Schlüssel der Zertifizierungsstelle.

# 6 Technische Sicherheitsmassnahmen

Die Anforderungen an technische Sicherheitsmassnahmen einer Zertifizierungsstelle bzw. einer Registrierungsstelle werden durch die angebotenen Dienstleistungen bestimmt. Das konkrete Sicherheitsniveau hinsichtlich der Grundwerte Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität wird in einem Sicherheitskonzept festgeschrieben. Das Sicherheitskonzept wird nicht veröffentlicht, aber im Rahmen der Konformitätsprüfung zur Verfügung gestellt.

Sofern in diesem CPS Anforderungen an einzelne Sicherheitsmassnahmen nicht spezifiziert werden, sind diese grundsätzlich an die entsprechenden Massnahmenkataloge des ISO/IEC 27001 anzulehnen.

## 6.1 Schlüsselerzeugung und Installation

### 6.1.1 Schlüsselerzeugung

Die Schlüsselpaare der Root-CA werden auf einem dedizierten HSM erzeugt. Das IT System, welches die Root-CA enthält, ist nicht an ein Netzwerk angeschlossen. Die Schlüssel werden ausschliesslich

auf einem HSM gespeichert und durch mehrere PED Keys (Schlüssel) gesichert. Ein Backup des HSM wird sicher aufbewahrt.

Die Schlüsselpaare der Issuing CAs werden in einem separaten HSM erzeugt und gespeichert und sind durch mehrere PED Keys gesichert. Ein Backup des HSM wird sicher aufbewahrt.

Die Schlüsselpaare der Zertifikatsstufen „Diamant“ und „Saphir“ werden ausschliesslich in SSCD erzeugt und aufbewahrt, die den Anforderungen des ZertES [1] oder mindestens FIPS 140-2 Level 3 entsprechen.

### 6.1.2 Übermittlung des privaten Schlüssels an den Zertifikatsinhaber

Schlüsselpaare für Signatur- und Authentisierungszertifikate der Klassen „Diamant“ und „Saphir“ werden ausschliesslich innerhalb eines SSCD erzeugt. Hält der Zertifikatsinhaber das Schlüsselpaar auf einem eigenen SSCD, wird ihm das SSCD auf geeignete Weise übergeben.

Zertifikate der Zertifikatsklassen „Rubin“ und „Smaragd“ werden durch die Registrierungsstelle erzeugt. Auf Wunsch des Kunden können Verschlüsselungs-Schlüssel so erstellt werden, dass das Schlüsselpaar in eine SmartCard importiert und im Falle eines Verlustes der SmartCard wieder hergestellt werden kann.

Soft-Zertifikate werden für den Fall, dass das Schlüsselpaar durch die Registrierungsstelle generiert wird, in einem verschlüsselten Container (PKCS#12) an den Inhaber übermittelt, wobei die PIN für die Entschlüsselung des Containers über einen separaten Weg zugestellt wird.

### 6.1.3 Auslieferung des öffentlichen Schlüssels an den Zertifikatausssteller

Die Registrierungsstellen, welche Zertifikate der Klassen „Diamant“ und „Saphir“ auf SSCD ausstellen, können Zertifikatsanforderungen nur über das von Swisscom zur Verfügung gestellte Frontend des Card Management Systems einreichen. Das Card Management System stellt sicher, dass der Public Key in einem PKCS#10 Request signiert und über eine sichere Verbindung an Swisscom geliefert wird.

### 6.1.4 Auslieferung des öffentlichen CA-Schlüssels

Alle Teilnehmer des Swisscom Digital Certificate Services können die öffentlichen Signaturprüf-schlüssel (public key) der Swisscom Root-CA und der untergeordneten CAs im PKCS#7-Format oder in binärer Form (DER) über den Verzeichnisdienst (siehe Kapitel 2.1) abrufen.

### 6.1.5 Schlüssellängen

Die eingesetzten kryptografischen Algorithmen und deren Schlüssellängen orientieren sich an den im TAV [3] referenzierten Veröffentlichungen der ETSI und sind momentan:

Root CA 2 (OID 2.16.756.1.83.10)

- RSA 4096 SHA-256 für den CA 2 Root-Key
- RSA 2048 SHA-256 für die CAs der nachfolgenden Stufe (Level 1)
- RSA 2048 SHA-256 für die Zertifikate mit der Bezeichnung CA 2 oder CA 3
- ECC 256 NIST-P256r1 für die Zertifikate mit der Bezeichnung Rubin CA 3

### 6.1.6 Parameter der öffentlichen Schlüssel und Qualitätssicherung

Die Parameter richten sich nach den Vorgaben der TAV [3] und werden von der CA erzeugt. Die Parameter werden bei ihrer Erzeugung sorgfältig ausgewählt.

### 6.1.7 Verwendungszweck der Schlüssel und Beschränkungen

Verwendungszweck der Schlüssel und Beschränkungen werden im entsprechenden X.509 v3 Feld (keyUsage) festgelegt (siehe Addendum zum CPS [8], Kapitel 2) und sind jeweils der entsprechenden CP zu entnehmen.

## 6.2 Schutz des privaten Schlüssels

Der private Schlüssel der Root-CA und der CAs der nachfolgenden Stufe (Level 1) werden in den HSMs erzeugt und abgelegt. Signaturen werden in den HSMs durchgeführt und der jeweilige private Schlüssel verlässt nie ein HSM.

Private Schlüssel der Zertifikatsklassen „Diamant“ und „Saphir“ werden in einem SSCD erzeugt und abgelegt. Signaturen werden im SSCD durchgeführt. Die eingesetzten SSCD entsprechen den Anforderungen der TAV [3].

Für den qualifizierten Signaturschlüssel wird auf dem SSCD eine spezielle Umgebung erstellt und Verfahren verwendet, die garantieren, dass der private Schlüssel angemessen geschützt und unter der alleinigen Kontrolle des Zertifikatinhabers ist.

### 6.2.1 Standard der kryptografischen Module

Die eingesetzten HSM-Module und SSCD für die Zertifizierung, genügen den Anforderungen der TAV [3]:

- HSM: SafeNet Luna SA
  → FIPS 140-2 Level 3

### 6.2.2 Teilung des privaten Schlüssels

Eine Teilung der privaten Schlüssel der Swisscom Root-CA und der Issung CA ist nicht vorgesehen.

### 6.2.3 Hinterlegung privater Schlüssel

Eine Hinterlegung privater Schlüssel von Zertifikatsinhabern ist nicht statthaft und findet für qualifizierte Signaturschlüssel nicht statt. Dasselbe gilt für Signaturschlüssel der Zertifikatsklasse „Saphir“.

Für alle anderen Klassen kann auf Wunsch des Zertifikatsinhabers eine Schlüsselhinterlegung angeboten werden.

### 6.2.4 Backup der privaten Schlüssel

Ein Backup der privaten Schlüssel der Zertifikatsklassen „Diamant“ und „Saphir“ bei der Verwendung von Smart Cards ist nicht möglich.

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

Von den Schüsselpaaren der Root-CA und der Issuing CAs werden Kopien angefertigt und auf einem HSM in einem Safe aufbewahrt. Die HSMs sind durch spezielle PED Keys (Schlüssel) gesichert.

### 6.2.5 Archivierung der privaten Schlüssel

Eine Archivierung der privaten Signatur und Authentisierungs-Schlüssel von Zertifikatsinhabern der Zertifikatsklassen „Diamant“ und „Saphir“ findet nicht statt.

### 6.2.6 Erstellung und Speicherung privater Schlüssel

Signatur- und Authentisierungs-Schlüssel der Klassen „Diamant“ und „Saphir“ sowie die CA Schlüssel werden ausschliesslich in kryptografischen Modulen (HSM und SmartCards) erstellt und gespeichert.

### 6.2.7 Aktivierung der privaten Schlüssel

#### 6.2.7.1 Zertifikat und privater Schlüssel auf eigenem SSCD

Die Aktivierung des privaten Schlüssels erfolgt durch die Eingabe von Aktivierungsdaten (z.B. PIN) durch den Zertifikatsinhaber.

#### 6.2.7.2 Zertifikat und privater Schlüssel im All-in Signing Service

Die Übergabe der Aktivierungsdaten entfällt. Die Willensbekundung zur Benutzung des privaten Schlüssels erfolgt über geeignete Mittel (z.B. Mobile ID [11]).

#### 6.2.7.3 Private Schlüssel der CAs

Zur Aktivierung der privaten Schlüssel der Issuing CAs wird der schwarze PED Key (Schlüssel) verwendet. Dieser PED Key befindet sich im Besitz der Rolle „Security Device Administrator (SDADM)“. Eine Aktivierung kann nur im Beisein einer zweiten Person, die im Besitz eines weiteren PED-Keys ist (vier-Augen-Prinzip), stattfinden.

### 6.2.8 Deaktivierung der privaten Schlüssel

Die Deaktivierung eines privaten Schlüssels erfolgt durch das Entfernen von Aktivierungsdaten (z.B. PIN) durch den Zertifikatsinhaber.

### 6.2.9 Vernichtung der privaten Schlüssel

Bei der Vernichtung der privaten Schlüssel der Root-CA und der ihr nachgelagerten Issuing CAs wird nach dem vier-Augen-Prinzip verfahren. Verantwortlich für die Vernichtung sind die Rollen ISO und SDADM.

### 6.2.10 Güte des kryptografischen Moduls

Siehe Kapitel 6.2.1.

## 6.3 Weitere Aspekte des Schlüsselmanagements

### 6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel werden sowohl im Verzeichnisdienst als auch auf Medien für die Datensicherung archiviert.

### 6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Die von der Root-CA und den CA-Services ausgestellten Zertifikate haben folgende Gültigkeitszeiträume:

- Zertifikat der Root-CA maximal 20 Jahre
- Zertifikate der nachgelagerten Issuing CAs maximal 10 Jahre
- Zertifikate der Klassen „Diamant“, „Saphir“ und „Smaragd“ maximal 3 Jahre

- Zertifikate der Klasse „Rubin“ maximal 5 Jahre

Die zulässige Nutzungsdauer von Schlüsselpaaren entspricht grundsätzlich der Gültigkeitsdauer der darauf basierenden Zertifikate. Eine Verwendung von vorhandenen Schlüsselpaaren im Rahmen einer Re-Zertifizierung ist nur zulässig, wenn die empfohlenen Algorithmen und Schlüssellängen dies erlauben (siehe Kapitel 6.1.5 und jeweils zugehörige CP, Kapitel 4.7.1).

## 6.4 Aktivierungsdaten

Für PINs zur Aktivierung von privaten Schlüsseln auf persönlichen SSCD dürfen keine trivialen Kombinationen gewählt werden. Die PINs sollten sowohl alphanumerische Zeichen als auch Sonderzeichen beinhalten und mindestens 6 Zeichen lang sein.

### 6.4.1 Schutz der Aktivierungsdaten

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

   Aktivierungsdaten müssen geheim gehalten werden. Für die Zertifikatsklasse „Diamant“ wird der Schlüssel nach 4 falschen Eingaben gesperrt.

   Für die Zertifikatsklasse „Saphir“ müssen inkorrekte und aufeinander folgende Aktivierungsversuche festgestellt werden können und nach einer im Voraus festgelegten Anzahl von Fehlversuchen der Gebrauch des Signaturschlüssels gesperrt werden.

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

   Die Übergabe der Aktivierungsdaten entfällt. Die Willensbekundung zur Benutzung des privaten Schlüssels erfolgt über geeignete Mittel (z.B. Mobile ID [11]).

## 6.5 Sicherheitsmassnahmen für Computer

### 6.5.1 Spezifische Anforderungen an technische Sicherheitsmassnahmen

Alle Anwendungen innerhalb der CA werden ausschliesslich auf Basis von gehärteten Betriebssystemen (sicherheitsoptimierte Betriebssysteme) betrieben. Für die CA und den Directory Service wird zusätzlich eine Change Auditing Software eingesetzt, welche einen Hash-Wert über die Konfigurationsfiles legt und somit Veränderungen feststellen kann.

Darüber hinaus werden folgende Sicherheitsmassnahmen umgesetzt:

- Restriktive Zugriffskontrolle,
- Benutzerauthentisierung und -autorisierung nach den „need-to-know“ und „need-to-do“ Prinzipien,
- Nachvollziehbarkeit durch Log-Files und eine gemeinsame, vertrauenswürdige Zeitbasis für alle Systeme der CA.

### 6.5.2 Güte /Qualität der Sicherheitsmassnahmen

Die Sicherheitsmassnahmen werden periodisch überprüft.

## 6.6 Lebenszyklus der Sicherheitsmassnahmen

### 6.6.1 Softwareentwicklung

Der Einsatz von Software (Eigen- oder Fremdentwicklung) erfolgt erst nach Abnahme und Freigabe.

### 6.6.2 Sicherheitsmanagement

Das Sicherheitsmanagement umfasst folgende Aspekte:

- Jährliches Audit (Konformitätsprüfung durch interne und externe Prüfer),
- Regelmässige Evaluierung und Weiterentwicklung des Sicherheitskonzepts (jährlich),
- Überprüfung der Sicherheit im laufenden Betrieb (siehe auch Kapitel 5.4),
- Regelmässige Integritätsprüfungen der eingesetzten Anwendungen und Betriebssysteme,
- Zentrales Logging aller sicherheitsrelevanten Vorgänge,
- Zusammenarbeit mit dem Swisscom-CERT,
- Einspielung von Upgrades und Patches, sofern erforderlich,
- Einsatz auf einem Produktivsystem erst nach Freigabe auf einem Testsystem.

## 6.7 Sicherheitsmassnahmen für das Netzwerk

Das Netzwerk der CA ist in verschiedene Sicherheitszonen unterteilt, die jeweils durch eine Firewall voneinander abgeschottet sind. Darüber hinaus werden zur Abwehr von Angriffen aus dem Internet, wie auch aus dem Intranet, Intrusion Prevention bzw. Detection Systeme eingesetzt. Kritische Sicherheitsvorfälle werden unverzüglich in Zusammenarbeit mit dem Swisscom-CERT verfolgt und bearbeitet.

## 6.8 Zeitstempel

Swisscom stellt einen Zeitstempeldienst gemäss Anforderungen in Ziffer 2.4 TAV [3] zur Verfügung.

Als Zeitbasis kommt eine Appliance von Meinberg zum Einsatz, welche über eine GPS – Aussenantenne synchronisiert und mittels DCF-77 Signal verifiziert wird. Die Zeitbasis wird über das Network Time Protocol (NTP) an alle Server der Swisscom Digital Certificate Service Infrastruktur verteilt.

Der Zeitstempeldienst wird auf dem HSM der Issuing CA bedient, somit wird er auf einem SafeNet Luna SA System bereitgestellt. Siehe CP des Zeitstempeldienstes für weitere Details.

# 7 Profile für Zertifikate, Widerrufslisten und Online-Statusabfragen

Profile für Zertifikate, Widerrufslisten (CRL) und Online-Statusabfragen (OCSP) sind entsprechend den Vorgaben des ZertES [1], den TAV [3] sowie den anderen referenzierten Dokumenten aufgebaut und im Addendum zu dieser CPS [8] detailliert beschrieben.

Weitere Details zu den Zertifikatsprofilen und -erweiterungen sind der jeweiligen CP, Kapitel 7, zu entnehmen.

# 8 Konformitätsüberprüfung (Compliance Audit) und andere Prüfungen

Die Regelungen sind der zugehörigen CP zu entnehmen.

# 9 Rahmenvorschriften

## 9.1 Gebühren

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

## 9.2 Versicherung

### 9.2.1 Versicherungsschutz

Der Versicherungsschutz der Swisscom erstreckt sich auf die gesetzlichen Haftpflichtansprüche gemäss Art. 3 Abs. 1 Bst. f ZertES [1]. Für die erwähnten Schäden und Kosten gilt eine gemeinsame Sublimite von CHF 2 Mio. pro Ereignis und CHF 8 Mio. pro Versicherungsjahr.

Ansonsten gelten die Allgemeinen Geschäftsbedingungen „Geschäftskunden“ von Swisscom (Schweiz) AG (AGB).

### 9.2.2 Versicherungsschutz für Zertifikatinhaber und RAs

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

## 9.3 Vertraulichkeit von Geschäftsinformationen

### 9.3.1 Vertraulich zu behandelnde Daten

Jegliche Informationen über Teilnehmer und Antragsteller, die nicht unter Kapitel 9.3.2 fallen, werden als vertrauliche Informationen eingestuft. Zu diesen Informationen zählen u.a. Geschäftspläne, Vertriebsinformationen, Informationen über Geschäftspartner und ebenso alle Informationen, die im Registrierungsprozess erfasst wurden.

### 9.3.2 Nicht vertraulich zu behandelnde Daten

Jegliche Informationen, die in den herausgegebenen Zertifikaten und der Liste der für ungültig erklärten Zertifikate explizit (z.B. Elemente des DN) oder implizit (z.B. Daten über die Zertifizierung) enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft.

### 9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Swisscom trägt die Verantwortung für 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 mit den Aufgaben betrauten Mitarbeiter auf Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet wurden.

Nicht als Dritte gelten die RA-Vertragspartner, welche im Rahmen der Bearbeitung des Zertifikatantrages Daten an Swisscom weitergeben können und an welche Swisscom wiederum die bearbeiteten Daten weitergeben kann. Zu Auditions- oder Revisionszwecken können Dokumente im

Beisein des Information Security Officers der Swisscom Digital Certificate Services oder eines namentlich benannten Vertreters eingesehen werden.

### 9.4 Schutz von Personendaten (Datenschutz)

Swisscom erhebt, speichert und bearbeitet nur Daten, die für die Erbringung der Leistungen, für die Abwicklung und Pflege der Kundenbeziehung, namentlich die Gewährleistung einer hohen Leistungsqualität, für die Sicherheit von Betrieb und Infrastruktur sowie für die Rechnungsstellung benötigt werden.

Zur Verhinderung von Missbrauch der Daten durch Spam-Sender können insbesondere E-Mail-Informationen, sofern im Zertifikat enthalten, nur von authentisierten Benutzern abgefragt werden. Es werden keine E-Mail-Adressen an nicht registrierte Benutzer geliefert. Im LDAP Verzeichnis werden keine systematischen Wildcard Abfragen unterstützt.

#### 9.4.1 Verantwortlicher Umgang mit Personendaten

Swisscom und die von ihr beauftragten Registrierungsstellen halten sich insbesondere an folgende Grundsätze:

- Personendaten dürfen nur rechtmässig beschafft werden,
- Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein,
- Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 DSG),
- Mit Personendaten darf kein Handel betrieben werden (Art. 15 Abs. 1 ZertES [1]).

#### 9.4.2 Offenlegung im Rahmen von Gerichts- und Verwaltungsverfahren

Swisscom unterliegt schweizerischem Recht und muss ihre Kundendaten bei Vorlage entsprechender Entscheidungen an staatliche Organe in Übereinstimmung mit den geltenden Gesetzen freigeben.

#### 9.4.3 Andere Umstände einer Weitergabe von Daten an Dritte

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

### 9.5 Urheberrechte

Swisscom ist Eigentümerin der Urheberrechte an folgenden Dokumenten:

- vorliegende CPS;
- dazugehörige CPs;
- dazugehörige Nutzungsbestimmungen.

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

## 9.6 Zusicherung und Gewährleistung

### 9.6.1 Verpflichtung der Swisscom

Swisscom verpflichtet sich als Anbieterin von Zertifizierungsdiensten alle im Rahmen dieser CPS und den zugehörigen CPs beschriebenen Aufgaben gemäss den Vorgaben des ZertES [1] und der Ausführungsbestimmungen (TAV [3]) durchzuführen.

### 9.6.2 Verpflichtung der RA-Vertragspartner

Die RA-Vertragspartner sind vertraglich verpflichtet, alle Anforderungen gemäss ZertES [1] und TAV [3], Ziffer 2.3.1 *„Registrierung, Verwaltung und Ungültigerklärung von Zertifikaten für Dritte“,* einzuhalten.

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

Bei einer RA, die Zertifikate der Zertifikatsklassen „Diamant“ ausgibt, wird die Einhaltung der Vorgaben (TAV [3]) von der Anerkennungsstelle überprüft.

### 9.6.3 Verpflichtung des Zertifikatinhabers

Bei Organisationszertifikaten ist die Organisation, auf deren Namen das Zertifikat im O-Feld ausgestellt ist, für den Erlass organisationsinterner Weisungen verantwortlich, die den Einsatz und den Zugang zum Zertifikat sowie dessen allfällige Sperrung regeln (z.B. Aufbewahrung der Smartcard, des Passwortes, des Sperrkennwortes usw.).

Des Weiteren gelten die Regelungen von Kapitel 4.5.1 der zugehörigen CP.

### 9.6.4 Verpflichtung des Zertifikatprüfers

Es gelten die Regelungen von Kapitel 4.5.2 der zugehörigen CP.

### 9.6.5 Verpflichtung anderer Teilnehmer

Sofern weitere Teilnehmer als Dienstleister in den Zertifizierungsprozess eingebunden werden, ist Swisscom in der Verantwortung, den Dienstleister zur Einhaltung der CPS und den zugehörigen CPs zu verpflichten.

## 9.7 Haftung von Swisscom

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

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

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

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

In allen anderen Fällen haftet Swisscom wie folgt:

- Bei Vertragsverletzungen haftet Swisscom für den nachgewiesenen Schaden, sofern sie nicht beweist, dass sie kein Verschulden trifft.
- Für absichtlich und grobfahrlässig verursachte Schäden haftet Swisscom unbegrenzt.
- Bei leichter Fahrlässigkeit haftet Swisscom für Personenschäden unbegrenzt, für Sach- und Vermögensschäden bis zu einem Betrag von CHF 5'000.- je Schadenereignis[3].

In keinem Fall haftet Swisscom für indirekte Schäden und Folgeschäden, insbesondere entgangenen Gewinn oder Daten- oder Reputationsverluste sowie Ansprüche Dritter.

## 9.8 Haftung des Zertifikatinhabers

Der Zertifikatsinhaber (bei Organisationszertifikaten die im O-Feld des Zertifikats genannte Organisation) ist für alle Handlungen, die mit dem Zertifikat gegenüber Dritten mit der Nutzung des Zertifikats begangen werden, verantwortlich. Für die Verwendung des dem Zertifikat zu Grunde liegenden geheimen Schlüssels haftet ausschliesslich der Zertifikatsinhaber (bei Organisationszertifikaten die im O-Feld des Zertifikats genannte Organisation).

## 9.9 Inkrafttreten und Aufhebung

### 9.9.1 Inkrafttreten

Diese CPS und die zugehörigen CPs treten an dem Tag in Kraft, an dem sie über den Informationsdienst (siehe Kapitel 2.2) der Swisscom Digital Certificate Services veröffentlicht werden.

### 9.9.2 Aufhebung

Dieses Dokument ist gültig bis 28.02.2018.

### 9.9.3 Konsequenzen der Aufhebung

Bei einer Aufhebung dieser CPS und den zugehörigen CPs sind die Zertifikatsinhaber für den Rest der Gültigkeitsdauer der bereits ausgestellten Zertifikate an die entsprechenden Nutzungsbedingungen gebunden.

## 9.10 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

Swisscom informiert die Zertifikatinhaber bei Kenntnis der E-Mail-Adresse via signierte E-Mail oder via Briefpost.

Die Kommunikation mit den übrigen Teilnehmern erfolgt mittels signierten Formularen via Email oder Brief. Ankündigungen und News werden auf der Homepage von Swisscom publiziert.

[3] Für die Zertifikate der Klassen „Diamant" gelten höhere Beträge, siehe zugehörige CP, Kapitel 9.7

## 9.11 Änderungen der Zertifizierungsrichtlinien

Kleinere Änderungen mit keiner oder minimaler Auswirkung auf die Benutzer werden durch Swisscom direkt in Kraft gesetzt. Grössere Änderungen werden in Absprache mit und nach Genehmigung durch die Anerkennungsstelle durchgeführt. Änderungen werden in einem Journal nachgeführt.

Werden Änderungen vorgenommen, die sicherheitsrelevante Aspekte betreffen oder die Abläufe seitens der in Kapitel 1.3 aufgeführten Beteiligten beeinflussen, werden diese umgehend informiert.

Die letztendliche Genehmigung der Richtlinien erfolgt durch das Governance Board.

## 9.12 Konfliktbeilegung

Im Konfliktfall bemühen sich die Beteiligten im Sinne von Kapitel 1.3 um eine einvernehmliche Streitbeilegung.

## 9.13 Anwendbares Recht und Gerichtsstand

Alle Rechtsbeziehungen im Zusammenhang mit den Services von Swisscom gemäss diesem Dokument unterliegen ausschliesslich Schweizer Recht, unter Ausschluss der Kollisionsnormen des internationalen Privatrechts und das Übereinkommen der Vereinten Nationen über den internationalen Warenkauf vom 11. April 1980.

Ausschliesslicher Gerichtsstand ist Bern, Schweiz.

## 9.14 Konformität mit dem geltenden Recht

Swisscom ist ein akkreditierter Anbieter von Zertifizierungsdiensten im Sinne des schweizerischen Signaturgesetzes ZertES [1] und stellt qualifizierte und fortgeschrittene Zertifikate aus.

## 9.15 Weitere Bestimmungen

### 9.15.1 Geltungsbereich

Alle in dieser CPS und den zugehörigen CPs enthaltenen Regelungen gelten zwischen Swisscom und den RA Partnern.

Die RA Partner sind verpflichtet, diese Regelungen ihrerseits entsprechend in die Verträge zwischen ihnen und den Zertifikatinhabern zu integrieren. Falls Swisscom mit den Zertifikatsinhabern direkt Verträge abschliesst, werden diese CPS und die CP der jeweiligen Zertifikatsklasse ebenfalls in die Verträge integriert.

### 9.15.2 Sprache

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

### 9.15.3 Gültigkeit

Dieses Dokument ist gültig bis 28.02.2018.

### 9.15.4 Übertragung der Rechte und Pflichten

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