



Swiss Post Platinum CP/CPS

Zertifizierungspolitik und Zertifizierungspraktiken (CP/CPS) der Swiss Post Platinum CA.

Document Type:	Zertifizierungspolitik und Zertifizierungspraktiken
OID:	2.16.756.1.89.1.1.1.4.3
Autoren:	Cavegn Aldo, Oechslin Barbara, Portmann Werner, Raemy Melanie
Klassifikation:	C1 (öffentlich)
Applicability:	Global
Owner:	CEO
Issue Date:	April 28 th , 2008
Version:	1.1.1
Obsoletes:	Version 1.0.6, April 1, 2008
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released
Überprüfung:	Dieses Dokument wird regelmässig, mindestens jedoch einmal pro Kalenderjahr, einer Überprüfung unterzogen. Für diese Überprüfung ist der Dokumentenverantwortliche zuständig.

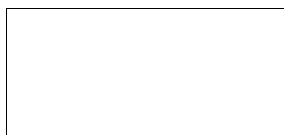
Haftungsausschluss: Die elektronische Version dieses Dokuments und alle darin enthaltenen Bestimmungen gelten als verbindlich, sofern sie im Adobe PDF-Format gespeichert und von zwei rechtmässigen Vertretern der SwissSign AG unterzeichnet sind. Alle anderen Kopien und Medien sind ungültig.

Versions Kontrolle

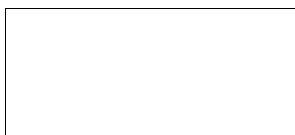
Datum	Version	Kommentar	Autor
05.01.07	1.0.1	Initial version	Melanie Raemy
15.01.07	1.0.2	Review	Mike Doujak
16.02.07	1.0.3	Einarbeitung Feedback Post	Melanie Raemy
07.03.07	1.0.4	Final review	Peter Delfosse
12.11.07	1.0.5	Repository-Links Modification	Philipp Zimmermann
20.02.08	1.0.6	Anpassung an neuen Registrierungsprozess und revidierte EIDI-V	Christoph Hofer
15.04.08	1.1.0	Review, Anpassung life cycle management	Björn Kanebog
20.04.08	1.1.1	Review	Michael Doujak

Authorisierung

Datum	Approved by	Approved by	Version
07.03.07	Peter Delfosse	Fredy Isler	1.0.4
21.11.07	Peter Delfosse	Fredy Isler	1.0.5
12.03.08	Adrian Humbel	Aldo Cavegn	1.0.6
28.04.08	Adrian Humbel	Aldo Cavegn	1.1.1



digital signature



digital signature

Inhaltsverzeichnis

1	Einleitung	7
1.1	Überblick	7
1.2	Titel und Identifikation des Dokumentes	7
1.3	PKI-Teilnehmer	8
1.3.1	Zertifizierungsstellen (Certification Authorities, CA)	8
1.3.2	Registrierungsstellen (Registration Authorities, RA)	8
1.3.3	Zertifikatsinhaber (Subscriber)	8
1.3.4	Zertifikatsprüfer (Relying Parties)	9
1.3.5	Weitere Teilnehmer (Other Participants)	9
1.4	Zertifikatsnutzung	9
1.4.1	Zulässige Zertifikatsnutzung	9
1.4.2	Unzulässige Zertifikatsnutzung	10
1.5	Verwaltung der CP/CPS	10
1.5.1	Für die Verwaltung zuständige Stelle	10
1.5.2	Ansprechpartner	10
1.5.3	Für die Feststellung der Eignung der CP/CPS und für die Verwaltung zuständige Stelle	10
1.5.4	Verfahren zur Genehmigung der CP/CPS	10
1.6	Definitionen und Abkürzungen	10
2	Dokumentenveröffentlichungs- und Verwaltungspflichten	14
2.1	Dokumentenverwaltung	14
2.2	Veröffentlichung der Zertifizierungsdaten	14
2.3	Zeitpunkt oder Häufigkeit der Veröffentlichung	14
2.4	Zugangskontrollen zur Dokumentenverwaltung	14
3	Identifikation und Authentisierung	15
3.1	Namen	15
3.1.1	Namensarten	15
3.1.2	Aussagekräftige Namen	16
3.1.3	Anonymität oder Pseudonyme der Zertifikatsinhaber	16
3.1.4	Regeln für die Auslegung unterschiedlicher Namensarten	16
3.1.5	Eindeutigkeit von Namen	16
3.1.6	Erkennung, Authentisierung und Rolle von Marken	16
3.2	Anfängliche Identitätsüberprüfung	16
3.2.1	Verfahren zum Nachweis des Besitzes eines Private Key	17
3.2.2	Authentisierung von Organisationen	17
3.2.3	Authentisierung von natürlichen Personen	17
3.2.4	Nicht überprüfte Informationen	18
3.2.5	Unterschriftsberechtigung	18
3.2.6	Kriterien für die gegenseitige Zertifizierung	18
3.3	Identifikation und Authentisierung für Anträge auf Zertifikatserneuerung	18
3.3.1	Identifikation und Authentisierung für Zertifikatserneuerung nach Ungültigerklärung	18
3.4	Identifikation und Authentisierung für Anträge auf Ungültigerklärung	18
4	Betriebsanforderungen für den Zertifikatslebenszyklus	19
4.1	Zertifikatsantrag	19
4.1.1	Wer kann einen Zertifikatsantrag einreichen	19
4.1.2	Registrierungsverfahren	19
4.2	Bearbeitung des Zertifikatsantrags	19
4.2.1	Durchführung von Identifikation und Authentisierung	19
4.2.2	Genehmigung oder Ablehnung von Zertifikatsanträgen	19
4.2.3	Dauer der Bearbeitung von Zertifikatsanträgen	20
4.3	Ausstellung von Zertifikaten	20
4.3.1	Von der CA bei der Zertifikatsausstellung durchgeführte Schritte	20
4.3.2	Benachrichtigung über die Zertifikatsausstellung	20

4.4	Annahme von Zertifikaten	20
4.4.1	Als Annahme des Zertifikats geltende Handlungen.....	20
4.4.2	Veröffentlichung des Zertifikats durch die CA.....	20
4.4.3	Benachrichtigung anderer Stellen durch die CA über die Zertifikatsausstellung.....	20
4.5	Nutzung von Schlüsselpaaren und Zertifikaten.....	20
4.5.1	Nutzung von Private Keys und Zertifikaten durch Zertifikatsinhaber.....	20
4.5.2	Nutzung von Public Keys und Zertifikaten durch Zertifikatsprüfer	20
4.6	Verlängerung von Zertifikaten (Certificate Renewal)	21
4.7	Zertifikatserneuerung (Certificate Re-Key)	21
4.8	Änderung von Zertifikaten	21
4.9	Ungültigerklärung und Suspendierung von Zertifikaten	21
4.9.1	Voraussetzungen für die Ungültigerklärung.....	21
4.9.2	Wer kann eine Ungültigerklärung beantragen	22
4.9.3	Verfahren zur Beantragung einer Ungültigerklärung	22
4.9.4	Frist für die Anträge auf Ungültigerklärung	22
4.9.5	Frist für die Bearbeitung der Anträge auf Ungültigerklärung durch die CA.....	22
4.9.6	Prüfpflichten der Zertifikatsprüfer in Bezug auf die Ungültigerklärung	22
4.9.7	Häufigkeit der CRL-Ausstellung	22
4.9.8	Maximale Verzögerung für CRLs.....	23
4.9.9	Option zur Online-Überprüfung von Ungültigerklärungen/Status.....	23
4.9.10	Anforderungen für die Online-Überprüfung von Ungültigerklärungen.....	23
4.9.11	Weitere verfügbare Optionen der Ungültigkeitsbekanntmachung	23
4.9.12	Besondere Anforderungen bei einer Verletzung des Schlüssels	23
4.9.13	Voraussetzungen für die Suspendierung.....	23
4.10	Dienste zum Zertifikatsstatus.....	23
4.11	Ende der Zertifikatsnutzung.....	23
4.12	Hinterlegung und Wiederherstellung von Schlüsseln	24
5	Einrichtung, Verwaltung und Betriebskontrollen	25
5.1	Physische Kontrollen.....	25
5.1.1	Lage und Beschaffenheit der Standorte.....	25
5.1.2	Physischer Zugang	25
5.1.3	Stromversorgung und Klimatisierung	25
5.1.4	Risiko eines Wassereintruchs	25
5.1.5	Brandschutz	25
5.1.6	Medienspeicherung.....	25
5.1.7	Abfallentsorgung.....	25
5.1.8	Entfernt gelagerte Backups	25
5.2	Verfahrenskontrollen	26
5.2.1	Vertrauenswürdige Rollen.....	26
5.2.2	Anzahl der pro Aufgabe erforderlichen Personen	26
5.2.3	Identifikation und Authentisierung für die einzelnen Rollen	26
5.2.4	Rollen mit getrennten Pflichten	26
5.3	Personalkontrollen.....	26
5.3.1	Qualifikation, Erfahrung, Überprüfungsanforderungen.....	26
5.3.2	Verfahren zur Überprüfung des Hintergrunds.....	27
5.3.3	Schulungsanforderungen.....	27
5.3.4	Häufigkeit der Fortbildung und Anforderungen	27
5.3.5	Häufigkeit und Abfolge von Stellenwechseln	27
5.3.6	Strafen für nicht autorisiertes Vorgehen.....	27
5.3.7	Anforderungen für unabhängige Vertragsnehmer	27
5.3.8	Dem Personal bereitgestellte Dokumentation.....	27
5.4	Verfahren zur Audit-Protokollierung	27
5.4.1	Art der aufgezeichneten Vorgänge.....	27
5.4.2	Häufigkeit der Protokollverarbeitung.....	28
5.4.3	Archivierungsdauer für das Auditprotokoll	28
5.4.4	Schutz des Auditprotokolls	28
5.4.5	Verfahren zum Backup des Auditprotokolls	28
5.4.6	Auditerfassungssystem (intern bzw. extern)	28
5.4.7	Benachrichtigung des den Vorgang verursachenden Inhabers	28
5.4.8	Bewertung von Sicherheitslücken.....	28
5.5	Archivierung von Aufzeichnungen	29
5.5.1	Art der archivierten Aufzeichnungen	29
5.5.2	Archivierungsdauer	29

5.5.3	Schutz des Archivs	29
5.5.4	Verfahren zum Backup des Archivs	29
5.5.5	Anforderungen für die Datierung der Aufzeichnungen	29
5.5.6	Archiverfassungssystem (intern bzw. extern).....	29
5.5.7	Verfahren zur Erlangung und Überprüfung archivierter Daten	29
5.6	Auswechseln der Schlüssel	29
5.7	Verletzungen und Wiederherstellung im Notfall	29
5.7.1	Verfahren zur Handhabung von Zwischenfällen und Verletzungen	29
5.7.2	Beschädigte Rechenressourcen, Software und/oder Daten.....	30
5.7.3	Verfahren bei kompromittierten privaten Schlüsseln	30
5.7.4	Geschäftskontinuität nach Notfällen.....	30
5.8	Beendigung der CA oder RA	30
6	Technische Sicherheitskontrollen.....	31
6.1	Erzeugung und Installation von Schlüsselpaaren	31
6.1.1	Erzeugung von Schlüsselpaaren	31
6.1.2	Bereitstellung des Private Key an den Zertifikatsinhaber	31
6.1.3	Bereitstellung des Public Key an den Zertifikatsaussteller	31
6.1.4	Bereitstellung des Public Key der CA an die Zertifikatsprüfer.....	31
6.1.5	Schlüssellänge.....	31
6.1.6	Erzeugung und Qualitätsprüfung von Public Key-Parametern	31
6.1.7	Verwendungszweck der Schlüssel (gemäss Feld «KeyUsage X.509 v3»)	31
6.2	Schutz der Private Keys und Kontrolle beim Erstellen von Verschlüsselungsmodulen	32
6.2.1	Standards und Kontrollen für Verschlüsselungsmodule.....	32
6.2.2	Kontrolle des Private Key durch mehrere Personen (M of N)	32
6.2.3	Hinterlegung des Private Key.....	32
6.2.4	Backup des Private Key.....	32
6.2.5	Archivierung des Private Key	33
6.2.6	Übertragung des Private Key an und von Verschlüsselungsmodule(n)	33
6.2.7	Speicherung des Private Key auf Verschlüsselungsmodulen	33
6.2.8	Verfahren zur Aktivierung des Private Key	33
6.2.9	Verfahren zur Deaktivierung des Private Key	33
6.2.10	Verfahren zur Vernichtung des Private Key	33
6.2.11	Einstufung der Verschlüsselungsmodule	33
6.3	Weitere Aspekte der Verwaltung von Schlüsselpaaren.....	34
6.3.1	Archivierung des Public Key	34
6.3.2	Nutzungszeiträume von Zertifikaten und Schlüsselpaaren	34
6.4	Aktivierungsdaten	34
6.4.1	Erzeugung und Installation von Aktivierungsdaten.....	34
6.4.2	Schutz der Aktivierungsdaten	34
6.4.3	Weitere Aspekte der Aktivierungsdaten	34
6.5	Sicherheitskontrollen der Computer	34
6.5.1	Spezifische technische Anforderungen für die Sicherheit der Computer	34
6.6	Technische Kontrollen zum Lebenszyklus	35
6.6.1	Systementwicklungssteuerung.....	35
6.6.2	Kontrollen zum Sicherheitsmanagement	35
6.6.3	Sicherheitskontrollen zum Lebenszyklus.....	35
6.7	Sicherheitskontrollen des Netzwerks	35
6.8	Datierung.....	35
7	Zertifikats-, CRL- und OCSP-Profil	36
7.1	Zertifikatsprofil	36
7.1.1	Zertifikatserweiterungen	36
8	Audit zur Einhaltung gesetzlicher Vorgaben und andere Beurteilungen	40
8.1	Häufigkeit oder Voraussetzungen der Beurteilung	40
8.2	Identität/Qualifikationen des Auditor	40
8.3	Beziehung des Auditor zur geprüften Stelle	40
8.4	Von der Beurteilung abgedeckte Themen	40
8.5	Bei einem Mangel getroffene Massnahmen	40
8.6	Mitteilung der Resultate	41

9	Sonstige geschäftliche und rechtliche Bestimmungen	42
9.1	Gebühren.....	42
9.2	Finanzielle Verantwortung	42
9.3	Vertraulichkeit von Geschäftsinformationen.....	42
9.4	Vertraulichkeit von Personendaten.....	42
9.5	Rechte des geistigen Eigentums	42
9.6	Zusicherungen und Gewährleistungen	42
9.6.1	Zusicherungen und Gewährleistungen der Zertifizierungsstelle (CA)	42
9.6.2	Zusicherungen und Gewährleistungen der Registrierungsstelle (RA)	42
9.6.3	Zusicherungen und Gewährleistungen des Zertifikatsinhabers.....	42
9.6.4	Zusicherungen und Gewährleistungen des Zertifikatsprüfers.....	43
9.6.5	Zusicherungen und Gewährleistungen anderer Teilnehmer	43
9.7	Gewährleistungsausschluss.....	43
9.8	Haftung	43
9.8.1	Haftung der SwissSign AG.....	43
9.8.2	Haftung des Zertifikatsinhabers	43
9.9	Schadenersatz	43
9.10	Inkrafttreten und Beendigung	43
9.10.1	Inkrafttreten.....	43
9.10.2	Beendigung	43
9.10.3	Wirkung der Beendigung.....	44
9.11	Einzelbenachrichtigungen und Mitteilungen an Teilnehmer	44
9.12	Änderungen	44
9.13	Beilegung von Streitigkeiten	44
9.14	Anwendbares Recht und Gerichtsstand.....	44
9.15	Einhaltung geltenden Rechts.....	44
9.16	Sonstige Bestimmungen.....	44
9.16.1	Abtretung.....	44
9.16.2	Salvatorische Klausel.....	44
9.16.3	Sprache	45

1 Einleitung

Das vorliegende Dokument enthält die Zertifizierungspolitik und die Zertifizierungspraktiken (Certificate Policy / Certification Practice Statement, nachfolgend CP/CPS) der „Swiss Post Platinum CA“, welche durch die SwissSign AG, einer Konzerngesellschaft der Schweizerischen Post (nachfolgend „Post“), im Auftrag der Post betrieben wird.

Die „Swiss Post Platinum CA“ ist eine unter der „SwissSign Platinum CA“ operierende Zertifizierungsstelle (nachfolgend „CA“). Die „SwissSign Platinum CA“ ist eine Root CA, welche in Übereinstimmung mit dem Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (nachfolgend „ZertES“) tätig ist. Für die Zertifizierungspolitik und Zertifizierungspraktiken dieser Root CA ist einzig das Dokument „SwissSign Platinum CP/CPS“ massgebend.

Die „Swiss Post Platinum CA“ stellt Zertifikate aus, welche ausschliesslich durch die Post unter dem Namen „PostZertifikat“ vertrieben werden. Die anwendbaren allgemeinen Geschäftsbedingungen der Post regeln Abschluss, Inhalt und Abwicklung von Verträgen zwischen der Post und ihren Kundinnen und Kunden über den Erwerb und den Einsatz von Postzertifikaten. Bei Widersprüchen mit dem vorliegenden Dokument gehen die allgemeinen Geschäftsbedingungen für Postzertifikate vor. Für alle von der „Swiss Post Platinum CA“ ausgestellten Zertifikate wird eine Gebühr erhoben, die durch die Post festgelegt wird.

Die „Swiss Post Platinum CA“ gibt ausschliesslich fortgeschrittene Zertifikate im Sinne von Art. 2 lit. b ZertES aus. Entsprechend handelt es sich bei diesen Zertifikaten nicht um qualifizierte Zertifikate im Sinne des ZertES.

Die „Swiss Post Platinum CA“ gibt, gestützt auf Art. 2 Abs. 2 EIDI-V (SR 641.201.1) und die technischen und administrativen Vorschriften (TAV) der Eidgenössischen Steuerverwaltung (ESTV) zur EIDI-V (SR 641.201.11/Anhang), fortgeschrittene Zertifikate für Organisationen aus, die über die notwendige Mehrwertsteuerkonformität verfügen.

In dieser CP/CPS bezieht sich der Ausdruck «diese CA» auf die „Swiss Post Platinum CA“.

1.1 Überblick

Diese CP/CPS der SwissSign AG für die „Swiss Post Platinum CA“ beschreibt:

- Die Zertifizierungspolitik dieser CA.
- Die Registrierungs politik der Registrierungsstellen der Schweizerischen Post für diese CA.
- Praktiken und Verfahren dieser CA.
- Praktiken und Verfahren der Registrierungsstellen für diese CA.
- Bestimmungen und Bedingungen, unter denen diese CA bereitgestellt wird.

Der Aufbau dieser CP/CPS richtet sich nach den Vorgaben des RFC 3647 (Request for Comments, Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework, 2003).

1.2 Titel und Identifikation des Dokumentes

Dieses Dokument trägt den Titel «Swiss Post Platinum CP/CPS», wie auf dem Deckblatt angegeben.

Die Objektidentifikationsnummer (OID) dieses Dokuments lautet:

OID 2.16.756.1.89.1.1.1.4.3

Die OID der SwissSign AG basiert auf der vom Schweizer Bundesamt für Kommunikation (BAKOM) zugewiesenen RDN und ist wie folgt aufgebaut:

1. Stelle	2. Stelle	3. Stelle	4. Stelle	5. Stelle	Bedeutung
2					Gemeinsamer ISO-CCITT-Baum
	16				Land
		756			Schweiz

1. Stelle	2. Stelle	3. Stelle	4. Stelle	5. Stelle	Bedeutung
			1		RDN
				89	SwissSign

Die Stellen 6 bis 9 der OID der SwissSign AG bezeichnen das Dokument. Stelle 10 gibt die Dokumentversion an und wird nur im Zertifikat des Zertifikatsinhabers angezeigt (siehe Kap. 7).

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (Certification Authorities, CA)

Die „Swiss Post Platinum CA“ ist die einzige von der SwissSign AG betriebene Zertifizierungsstelle, die Zertifikate unter dieser CP/CPS ausstellt.

1.3.2 Registrierungsstellen (Registration Authorities, RA)

Die unter diesem CP/CPS tätigen Registrierungsstellen (nachfolgend „RA“) werden ausschliesslich von der Schweizerischen Post oder von ihr ausgebildeten und autorisierten Dritten betrieben.

1.3.3 Zertifikatsinhaber (Subscriber)

Inhaber von durch diese CA ausgestellten Zertifikate können sowohl natürliche Personen als auch Organisationen sein. Die Beantragung eines Zertifikates setzt immer voraus, dass sich eine natürliche Person (Antragsteller) bei der Registrierungsstelle identifiziert und die geforderten Dokumente vorlegt.

Die Zertifikatsinhaber und Antragsteller haben insbesondere folgende Pflichten:

- Aneignung grundlegender Kenntnisse über die Nutzung von Public Key-Verschlüsselung und Zertifikaten;
- Bereitstellung vollständiger und korrekter Informationen im Registrierungsverfahren (insbesondere Registrierungsformular, Identitätsnachweis, allenfalls Belege zur Organisation);
- Nutzung der Zertifikate ausschliesslich für die vorgesehenen legalen und autorisierten Zwecke;
- Schutz des Private Key, der sicheren Signaturerstellungseinheit und der Aktivierungsdaten vor nicht autorisiertem Zugriff (insbesondere durch Nichtoffenlegung der Private Keys und Passwörter sowie der Vermeidung von leicht zu erratenden Passwörtern);
- Nutzung des Private Key ausschliesslich in sicheren Rechnerumgebungen, die von vertrauenswürdigen Quellen bereitgestellt wurden und durch modernste Sicherheitsmassnahmen geschützt werden;
- Benachrichtigung der Registrierungsstelle über jegliche Änderungen an den im Zertifikat enthaltenen Informationen bzw. über jegliche Änderungen an den äusseren Umständen, durch welche die Informationen im Zertifikat irreführend oder inkorrekt würden;
- Sofortige Benachrichtigung der Registrierungsstelle, falls eine vermutete oder tatsächliche Verletzung des Private Key vorliegt und Beantragung der Ungültigerklärung des Zertifikats;
- Sofortige Einstellung der Nutzung des Zertifikats im Falle (a) des Ablaufs oder der Ungültigerklärung des Zertifikats, (b) jeglicher vermuteter oder tatsächlicher Beschädigung/Beeinträchtigung oder c) jeglicher vermuteter oder tatsächlicher Kompromittierung des in dem Zertifikat dem Public Key entsprechenden Private Key und sofortige Entfernung des Zertifikats von den Geräten und/oder Softwareprogrammen, auf denen es installiert war;
- Nutzung des Zertifikats unter Anwendung der angebrachten Sorgfalt und unter Einhaltung geltender gesetzlicher und vertraglicher Vorschriften;
- Einholung aller für den Export, Import und/oder die Nutzung eines von dieser CA ausgestellten Zertifikats erforderlichen Lizenzen und Erlaubnisse.

1.3.4 Zertifikatsprüfer (Relying Parties)

Zertifikatsprüfer sind natürliche Personen oder Organisationen, welche Zertifikate zur Validierung von Signaturen und Überprüfung der Identität der Zertifikatsinhaber und/oder zur sicheren Kommunikation mit diesem Zertifikatsinhaber nutzen. Zertifikatsprüfer dürfen Zertifikate nur in Übereinstimmung mit den in dieser CP/CPS aufgeführten Bestimmungen und Bedingungen nutzen und sie müssen über grundlegende Kenntnisse über Public Key-Verschlüsselung und Zertifikate verfügen. Sie sind selbst dafür verantwortlich, die Gültigkeit der Zertifikate mit Hilfe geeigneter Verfahren sowie die anzuwendenden Richtlinien zu überprüfen.

Zertifikatsprüfer können gleichzeitig auch Zertifikatsinhaber im Rahmen dieser CA sein.

1.3.5 Weitere Teilnehmer (Other Participants)

Weitere Teilnehmer sind natürliche Personen oder Organisationen, die dem Zertifikat eines Zertifikatsinhabers vertrauen oder auf irgendeine Weise an der Erstellung von Zertifikaten beteiligt sind und eventuell die Identität der Zertifikatsinhaber überprüfen und/oder die Kommunikation mit diesem Zertifikatsinhaber absichern wollen.

Weitere Teilnehmer können gleichzeitig auch Zertifikatsinhaber im Rahmen dieser CA sein.

1.4 Zertifikatsnutzung

1.4.1 Zulässige Zertifikatsnutzung

Unter dieser CP/CPS werden die folgenden Zertifikate ausgestellt:

Zertifikate für natürliche Personen mit oder ohne Organisationsbezeichnung

Zertifikate für natürliche Personen werden ausschliesslich in einem Zertifikatsset ausgegeben (sogenanntes Triple-Key-Verfahren). Entsprechend werden folgende 3 Zertifikate von dieser CA als kombiniertes Paket ausgestellt:

- Ein Authentisierungszertifikat, bei dem im Feld KeyUsage die Bits digitalSignature und keyAgreement gesetzt sind und der Geltungsbereich des Zertifikats erweitert ist. Siehe auch Kapitel 6.1.7. Der entsprechende Private Key muss auf einer SSCD erstellt worden sein und darf nur einmal existieren.
- Ein Signaturzertifikat, bei dem im Feld KeyUsage das Bit nonRepudiation gesetzt ist. Siehe auch Kapitel 6.1.7. Der entsprechende Private Key muss auf einer SSCD erstellt worden sein und darf nur einmal existieren.
- Ein Verschlüsselungszertifikat, bei dem im Feld KeyUsage die Bits keyEncipherment und dataEncipherment gesetzt sind und der Geltungsbereich des Zertifikats erweitert ist. Siehe auch Kapitel 6.1.7. Es können zusätzliche Kopien des entsprechenden Private Key existieren. Die Verwendung einer SSCD ist optional.

Zertifikate für Organisationen

Zertifikate für Organisationen werden ausschliesslich in einem Zertifikatsset ausgegeben (sogenanntes Dual-Key-Verfahren). Entsprechend werden folgende 2 Zertifikate von dieser CA als kombiniertes Paket ausgestellt:

- Ein Signaturzertifikat, bei dem im Feld KeyUsage die Bits digitalSignature und nonRepudiation gesetzt sind und der Geltungsbereich des Zertifikats erweitert ist. Siehe auch Kapitel 6.1.7. Der entsprechende Private Key muss auf einer SSCD erstellt worden sein und darf nur einmal existieren.
- Ein Verschlüsselungszertifikat, bei dem im Feld KeyUsage die Bits keyEncipherment und dataEncipherment gesetzt sind und der Geltungsbereich des Zertifikats erweitert ist. Siehe auch Kapitel 6.1.7. Es können zusätzliche Kopien des entsprechenden Private Key existieren. Die Verwendung einer SSCD ist optional.

Signatur- und Authentisierungszertifikate dürfen nicht zur Verschlüsselung, Verschlüsselungszertifikate nicht zur Signierung oder Authentisierung verwendet werden.

Bei sämtlichen von dieser CA ausgegebenen Zertifikaten handelt es sich um fortgeschrittene Zertifikate. Diese Zertifikate können folglich nicht zum digitalen Signieren gemäss Artikel 14 Abs. 2^{bis} OR (Schweizer Obligationenrecht) eingesetzt werden. Postzertifikate für Organisationen sind konform mit der Verordnung des Eidgenössischen Finanzdepartements über elektronische Daten und Informationen (EIDI-V, SR 641.201.1) sowie der technischen und administrativen Vorschriften (TAV) der Eidgenössischen Steuerverwaltung (ESTV) zur EIDI-V (SR 641.201.11/Anhang).

1.4.2 Unzulässige Zertifikatsnutzung

Jegliche von Kapitel 1.4.1 abweichende Nutzung ist untersagt.

1.5 Verwaltung der CP/CPS

1.5.1 Für die Verwaltung zuständige Stelle

Die Swiss Post Platinum CP/CPS wurde von der SwissSign AG erstellt und wird von ihr aktualisiert.

SwissSign AG
Pfungstweidstrasse 60b
8080 Zürich
Switzerland
Tel.: +41 (58) 386 24 88

Aktuelle Versionen der Dokumente können von der SwissSign-Website heruntergeladen werden (<http://repository.swissign.com>).

Die aktuelle Version des CP/CPS-Dokuments muss von zwei Bevollmächtigten der SwissSign AG digital signiert sein und ist die einzige verlässliche Quelle für die „Swiss Post Platinum CP/CPS“.

1.5.2 Ansprechpartner

Die folgende Person ist der Hauptansprechpartner für sämtliche Fragen oder Anregungen in Hinblick auf die „Swiss Post Platinum CP/CPS“.

Aldo Cavegn
Produkt Manager PostZertifikat
csp.feedback@swissign.com

Positive wie negative Rückmeldungen sind stets willkommen und an die oben angegebene E-Mail-Adresse zu richten, um ihre angemessene und rechtzeitige Bearbeitung zu gewährleisten.

1.5.3 Für die Feststellung der Eignung der CP/CPS und für die Verwaltung zuständige Stelle

Die Unternehmensleitung der SwissSign AG bereitet Entscheidungen über die Eignung und Anwendbarkeit dieser CP/CPS vor. Die Post entscheidet die Freigabe des CP/CPS.

1.5.4 Verfahren zur Genehmigung der CP/CPS

Die Genehmigung der CP/CPS erfolgt durch die Bevollmächtigten der SwissSign AG nach Rücksprache mit der Schweizerischen Post.

1.6 Definitionen und Abkürzungen

Begriff	Abkürzung	Definition
Fortgeschrittene elektronische Signatur		Eine elektronische Signatur im Sinne von Art. 2 lit. b ZertES, welche dem Inhaber zugeordnet werden kann und seine Identifikation ermöglicht. Sie wird mit Mitteln erstellt, die der alleinigen Kontrolle des Inhabers unterstehen, und macht jegliche Änderung des zugeordneten Datensatzes ersichtlich.

Begriff	Abkürzung	Definition
Algorithmus		Arbeitsanweisung um eine Aufgabe zu lösen. Ein Verschlüsselungsalgorithmus ist ein mathematischer Prozess, um Mitteilungen zu verschlüsseln und zu entschlüsseln.
Attribut		An einen Zertifikatsinhaber gebundene Informationen, die ein Merkmal dieses Zertifikatsinhabers, wie z. B. Zugehörigkeit zu einer Gruppe oder Rolle bestimmen.
Authentisierung		Authentisierung ist ein Prozess zur Identifikation von Zertifikatsinhabern. Benutzername und Passwort ist die gebräuchlichste Methoden der Authentisierung
CA Operator	CAO	Eine für den Betrieb der CA einschliesslich der Festlegung von Zertifikatsparametern für RA und RAO gemäss der Zertifikatspolitik verantwortliche Person.
Zertifikat		Elektronische Bescheinigung, die einen Public Key mit dem Namen einer Person oder Organisation verknüpft. Enthält mindestens ein Subjekt, eine eindeutige Seriennummer, einen Aussteller und eine Gültigkeitsperiode.
Anbieterin von Zertifizierungsdiensten (CSP) oder Zertifizierungsstelle (CA)	CSP, CA	Stelle, die im Rahmen einer elektronischen Umgebung Daten bestätigt und zu diesem Zweck digitale Zertifikate ausstellt, signiert, für ungültig erklärt und verwaltet.
Zertifikatserweiterung		Optionale Felder in einem Zertifikat.
Zertifizierungspolitik	CP	Richtlinien, die einerseits eingehalten werden müssen, damit ein Zertifikat ausgegeben wird und andererseits nach Ausgabe eingehalten werden müssen.
Zertifikatsstatus	CRL	Eine Liste der für ungültig erklärten Zertifikate
Zertifizierungspraktiken	CPS	Dokument, das die Rechte und Verantwortungen aller beteiligten Parteien regelt (Registrierungsstelle, Zertifizierungsstelle, Verzeichnisdienst, Zertifikatsprüfer)
Elektronische Signatur		Bei einer elektronischen Signatur handelt es sich um Verfahren das mit Hilfe von elektronischen Daten, die Authentizität und Integrität von elektronischen Informationen, meist elektronischen Dokumenten, sicherstellen sollen.
Distinguished Name	DN	-> Subject
Digitale Signatur		-> Elektronische Signatur
Allgemeine Geschäftsbedingungen	AGB	Vertragliche Vereinbarung zwischen der Post und dem Kunden.
HTTP	HTTP	Hypertext Transfer Protocol. HTTP wird dazu verwendet um Webseiten und andere Daten aus dem Web (WWW) in einen Webbrowser zu laden.
HTTPS	HTTPS	Sicheres Hyper-Text Transfer Protocol verwendet SSL
Schlüssel		-> Private Key, Public Key
Lightweight Directory Access Protocol	LDAP	Lightweight directory access protocol. Wird dazu verwendet, um Daten aus einem öffentlichen Verzeichnis zurückzuholen.
LDAP Secure	LDAPS	LDAP gesichert mit SSL
Online Certificate Status Protocol	OCSP	Online Certificate Status Protocol: Methode zur Verifizierung in Echtzeit, ob ein Zertifikat gültig ist.
PKCS		PKCS bezieht sich auf eine Reihe von Verschlüsselungsstandards für Public Keys (Public Key Cryptography Standards), die von den RSA Laboratories entwickelt und veröffentlicht werden.
Private Key		Einer von zwei in der Public Key-Kryptografie verwendeten Schlüssel. Der Private Key ist nur dem Zertifikatsinhaber bekannt und wird verwendet, um Mitteilungen zu signieren oder zu entschlüsseln.

Begriff	Abkürzung	Definition
Public Key		Der öffentliche Schlüssel eines Public-Private-Key-Kryptographiesystems. Dieser Schlüssel wird verwendet zur Prüfung von "Signaturen" (-> elektronische Signatur) auf eingehenden Mitteilungen und zur Verschlüsselung einer Datei oder Mitteilung, so dass einzig der Eigentümer des Private Key die Datei oder Mitteilung entschlüsseln kann.
Public Key Infrastructure	PKI	Prozesse und Technologien zur Ausstellung und Verwaltung von digitalen Identitäten zur Verwendung durch Drittpersonen, um natürliche Personen oder Organisationen zu authentisieren.
RA Operator	RAO	Die für die Identifikation des Antragstellers verantwortliche Person, welche die Nachweise der Identität entgegennimmt, den CSR autorisiert und den autorisierten CSR an die CA weiterleitet.
Zertifikatsprüfer		Prüfer eines Zertifikats, der im Vertrauen in das Zertifikat agiert und/oder Unterschriften mit Hilfe des Zertifikats prüft.
Antragsteller		Antragsteller sind natürliche Personen oder Organisationen, die ein Zertifikat beantragen, aber noch nicht erhalten haben.
RSA		Public Key-Verschlüsselungsalgorithmus
SSL		Secure Sockets Layer. Ein von Netscape entwickeltes Protokoll, das sichere Transaktionen über das Internet ermöglicht. URLs die eine SSL-Verbindung erfordern, beginnen mit https: anstelle von http:.
Subject	DN	Felder des Zertifikats, welche den Zertifikatsinhaber identifiziert. Auch referenziert als Distinguished Name (DN). Beispiele: /CN=John Doe /Email=jd@signdemo.com /CN=pseudo: Marketing /O=SwissSign AG /C=CH /Email=marketing@signdemo.com /CN=John Doe /O=SwissSign AG /OU=DEMO/C=CH /Email=john.doe@signdemo.com /CN=swiss.signdemo.com /O=SwissSign AG /OU=DEMO /C=CH /Email=root@signdemo.com obligatorisch Felder im Subject: Common Name --- /CN Email address --- /Email optionale Felder im Subject: Organization --- /O Organizational Unit --- /OU Domain Component --- /DC Country Name --- /C Locality Name --- /L Street Address --- /STREET Given Name --- /G Surname --- /S Initials --- /I Unique Identifier --- /UID Serial Number --- /SN Title --- /T Description --- /D
Zertifikatsinhaber (Subscriber)		Zertifikatsinhaber sind natürliche Personen oder Organisationen, die im Zertifikat als solche ausgewiesen sind.
TAV-BAKOM		Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur, SR 943.032.1.
2-Faktor-Authentisierung		Eine 2-Faktor-Authentisierung ist ein beliebiges Authentisierungsprotokoll, das zwei unabhängige Verfahren zur Feststellung von Identität und Rechten erfordert.
Uniform Resource Locator	URL	Uniform Resource Locator. Die globale Adresse eines Dokuments und anderer Ressourcen auf dem WWW, z.B. http://swissign.com. Der erste Teil bezeichnet das zu benutzende Protokoll (http) und der zweite Teil zeigt die Domain, wo das Dokument zu finden ist.
USB Token		Eine sichere Signaturerstellungseinheit, die wie ein gewöhnlicher USB Memory Stick aussieht. Sie ist vor Eingriffen geschützt und dient zur sicheren Speicherung und Nutzung von Private Keys.
VZertES		Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur, SR 943.032.

Begriff

ZertES

Abkürzung Definition

Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur, SR 943.03.

2 Dokumentenveröffentlichungs- und Verwaltungspflichten

Die SwissSign AG wird ihre Zertifikate, CP/CPS, CRL und dazugehörige Dokumente für diese CA auf den Websites swissign.com oder swissign.net öffentlich zugänglich machen. Um die Integrität und Authentizität zu gewährleisten müssen alle Dokumente digital signiert sein. Zum Nachweis des Geltungszeitraums der Dokumente ist eine Versionsübersicht enthalten.

2.1 Dokumentenverwaltung

Die SwissSign AG verwaltet die Dokumentation in Zusammenhang mit allen ihren CAs auf den Websites swissign.com und swissign.net. Die Websites sind miteinander verknüpft um eine nahtlose Navigation zu ermöglichen.

Die SwissSign AG unterhält zwei Websites um die allgemeine Sicherheit der Lösung zu erhöhen:

swissign.net: Diese Website wird für alle Funktionen in Zusammenhang mit den Zertifikaten (CRL, LDAP etc.) genutzt. Der Zugang der Mitarbeiter von SwissSign zu dieser Website ist streng geregelt (rollenbasierte Zugriffskontrolle) und die Kodierung ist so sicher wie möglich ausgeführt.

swissign.com: Diese Website wird für die Verbreitung von Informationen genutzt. Hier sind Informationen zu den Produkten und dem Unternehmen zu finden. Der Zugang der Mitarbeiter von SwissSign zu dieser Website unterliegt nicht dem allgemeinen Rollenmodell, da alle wichtigen Inhalte (Dokumente) aus digital signierten Dokumenten bestehen.

Verschiedene Informationen und Dokumentationen zu dieser CA und der von ihr ausgegebenen Zertifikaten (wie AGB, Antrag, Erneuerung, Ungültigerklärung, Download) werden auf der Website der Post (www.postzertifikat.ch) publiziert.

2.2 Veröffentlichung der Zertifizierungsdaten

Dieses Kapitel wird im SwissSign Platinum CP/CPS spezifiziert.

Zusätzlich gilt, dass Post RA die SwissSign CA anweist, welche Zertifikate für den öffentlichen Zugang freigegeben sind.

2.3 Zeitpunkt oder Häufigkeit der Veröffentlichung

Dieses Kapitel wird im SwissSign Platinum CP/CPS spezifiziert.

Zusätzlich werden Zeitpunkt und Häufigkeit der Veröffentlichung der Dokumente der Post RA wie folgt geregelt:

Die aktuellste Version der AGB ist immer unter www.postzertifikat.ch abrufbar.

2.4 Zugangskontrollen zur Dokumentenverwaltung

Dieses Kapitel wird im SwissSign Platinum CP/CPS spezifiziert.

Zusätzlich wird der Zugang zur Webseite der Post wie folgt geregelt:

Schreibzugriff zum Webserver RA Post erhalten nur Mitarbeiter der RA Post, welchen die Rolle Systemadministrator zugeteilt wurde. Der Zugriff ist mittels Benutzername und Passwort geschützt.

Mitarbeiter in der Rolle RAO haben Lesezugriff auf den Webserver RA Post. Dieser Zugang ist mittels starker Authentisierung via Zertifikat geschützt.

3 Identifikation und Authentisierung

3.1 Namen

3.1.1 Namensarten

3.1.1.1 Natürliche Personen

Der Distinguished Name (DN) in einem von der „Swiss Post Platinum CA“ ausgestellten Zertifikat entspricht dem Standard X.500.

Für den Distinguished Name sind mindestens zwei Felder erforderlich. Diese müssen /CN= und /Email= sein, wobei /Email=«E-Mail-Adresse» lautet.

Bei Zertifikaten für natürliche Personen werden Namen angegebenen als /CN=«Vorname», optional «weitere Vornamen», «Nachname».

Vorname, weitere Vornamen und Nachname im CN müssen exakt mit den Namen, die in der zur Identifikation vorgelegten Dokumentation angegebenen sind, übereinstimmen. Hat eine Person mehr als einen Vornamen, muss im Distinguished Name mindestens ein Vorname erscheinen. Mit Sonderzeichen wird gemäss Kapitel 3.1.4 verfahren. Kurzformen oder Rufnamen sind nicht zulässig. Aus mehreren Wörtern bestehende Namen sind zulässig.

Ein Name sowie die Daten zu seiner Identifikation müssen gemäss Kapitel 3.2.3 autorisiert werden.

SubjectAltName ist ein Pflichtfeld für an natürliche Personen ausgestellte Zertifikate und enthält eine exakte Kopie des E-Mail-Felds im Subject.

3.1.1.2 Natürliche Personen mit Organisationsbezeichnung

Es gelten die gleichen Regeln, wie für die natürlichen Personen.

Zudem sind die folgende zwei Felder gesetzt: /O= «Organisationsname» und /C=«Land».

Organisationsbezeichnung und Ländername müssen exakt mit den Namen, die in der zur Identifikation vorgelegten Dokumentation angegeben sind, übereinstimmen.

Die Namen und Daten zur Identifikation der Organisation müssen gemäss Kapitel 3.2.2 autorisiert werden.

3.1.1.3 Organisationen

Der Begriff Organisation umfasst juristische Personen des privaten und öffentlichen Rechts sowie Rechtsgemeinschaften, welche in eigenem Namen Rechte und Pflichten begründen können.

Der Distinguished Name (DN) in einem von der „Swiss Post Platinum CA“ ausgestellten Zertifikat entspricht dem Standard X.500.

Für den Distinguished Name werden folgende Felder gesetzt: /C=, /O=, /SP, /L, /CN= und optional /Email=.

Bei Zertifikaten für Organisationen werden Namen angegebenen als /CN=«Organisationsbezeichnung», /C=«Land», /O=«Organisationsbezeichnung» (gleich wie /CN), /SP=«Kanton», /L=«Gemeinde» und optional /Email=«E-Mail-Adresse».

Optional können noch mehrere Felder /OU= gesetzt werden, welche die Abteilung oder Filiale der Organisation beschreiben.

Organisationsbezeichnung und Ländername müssen exakt mit den Namen, die in der zur Identifikation vorgelegten Dokumentation angegeben sind, übereinstimmen.

Die Namen und Daten zur Identifikation müssen gemäss Kapiteln 3.2.2 und 3.2.3 autorisiert werden.

SubjectAltName ist ein optionales Feld für an Organisationen ausgestellte Zertifikate. Falls es vorhanden ist, enthält es eine exakte Kopie des E-Mail-Felds im Subject.

3.1.2 Aussagekräftige Namen

Der in einem Zertifikat enthaltene Name für Subject und Aussteller MUSS aussagekräftig sein, d.h. der RA liegen angemessene Belege für die bestehende Verbindung zwischen diesen Namen und den Personen, bzw. Organisationen, zu denen sie gehören, vor. Um dies zu erreichen muss die Verwendung eines Namens durch dessen rechtmässigen Inhaber oder einen Rechtsvertreter des rechtmässigen Inhabers autorisiert sein.

3.1.3 Anonymität oder Pseudonyme der Zertifikatsinhaber

Es gibt keine Möglichkeit, dass Zertifikatsinhaber anonym bleiben oder Pseudonyme verwenden können.

3.1.4 Regeln für die Auslegung unterschiedlicher Namensarten

Viele Sprachen enthalten Sonderzeichen, die von dem zur Definition des Subjekts im Zertifikat verwendeten ASCII-Zeichensatz nicht unterstützt werden. Zur Vermeidung von Problemen können lokale Ersetzungsregeln angewandt werden:

Grundsätzlich werden nationale Zeichen durch ihre ASCII-Entsprechung dargestellt, z.B. werden é, è, à, ç als e, e, a, c dargestellt.

Für die deutschen «Umlaute» kann ein gesondertes Verfahren angewandt werden: ä, ö, ü werden entweder als ae, oe, ue oder als a, o, u dargestellt.

3.1.5 Eindeutigkeit von Namen

Alle aus der „SwissSign Platinum CA – G2“ ausgestellten CAs garantieren die Eindeutigkeit des Inhalts des Subject Feldes in einer Art und Weise dass alle gültigen Zertifikate mit identischem Subject Feld dem selben Individuum oder der selben Organisation gehören. Die folgenden Regeln werden erzwungen:

- Alle Zertifikate für Individuen mit identischem Subject müssen dem selben Individuum angehören. Dies schliesst explizit abgelaufene oder für ungültig erklärte Zertifikate ein.
- Alle Organisationszertifikate mit identischem Subject müssen der selben Organisation gehören. Dies schliesst explizit abgelaufene oder für ungültig erklärte Zertifikate ein.

3.1.6 Erkennung, Authentisierung und Rolle von Marken

Die Post RA behalten sich das Recht vor, Zertifikatsanträge abzulehnen oder Zertifikate für ungültig zu erklären, falls diese anstössige, falsche oder irreführende Informationen enthalten oder gegen die Rechte von Dritten verstossen. Die Post RA ist, ausser beim Postzertifikat für Organisationen, nicht verpflichtet, die rechtmässige Verwendung von Namen und Marken zu überprüfen. Es ist in der alleinigen Verantwortung des Zertifikatsinhabers, die rechtmässige Verwendung gewählter Namen und Marken zu gewährleisten.

3.2 Anfängliche Identitätsüberprüfung

Die anfängliche Identitätsüberprüfung ist Teil des Antragsverfahrens für Zertifikate, wie in Kapitel 4.1 beschrieben.

3.2.1 Verfahren zum Nachweis des Besitzes eines Private Key

Die Post RA erzeugt in einem eigenen Prozess die Schlüsselpaare für den Antragsteller. Dieser Prozess garantiert die folgenden Eigenschaften:

- Jede sichere Signaturerstellungseinheit wurde original vom Hersteller geliefert und kann exakt ein einziges Mal genutzt werden.
- Jedes Schlüsselpaar für Authentisierung und digital Signatur wurde im SSCD erzeugt, ist einzigartig und kann nicht kopiert werden.
- Jedes SSCD ist mit einer Transportsicherung versehen, die dem Antragsteller auf einem sicheren Kanal übermittelt wird, die nur ein einziges Mal verwendet werden kann und die vor dem produktiven Einsatz des SSCD zwingend geändert werden muss.

3.2.2 Authentisierung von Organisationen

Bei ausreichender Autorisation durch die betreffende Organisation können Einzelpersonen den Namen einer Organisation im Zertifikat eintragen lassen.

Der DN eines Zertifikats, das von dieser CA ausgestellt wurde, kann eine Instanz des Organisationsattributs enthalten. Wenn der Antragsteller das Organisationsattribut zu einem Teil des DN machen will, sind folgende Regeln einzuhalten:

- Bei Verwendung des Unternehmensfelds ist die Verwendung des Länderfelds Pflicht.
- Der Registrierungsvorgang jeder unter dieser CP/CPS operierenden Registrierungsstelle muss Massnahmen zur Feststellung der Identität eines Unternehmens sowie zur Autorisation der Verwendung von dessen Namen umfassen.
- Der Antragsteller muss eine rechtsgültige Dokumentation über die Organisation vorlegen (z.B. Handelsregisterauszug, Gesellschaftsvertrag, Eintragungsbcheinigung der Eidgenössischen Steuerverwaltung usw.).
- Die Verwendung des Organisationsnamens muss von einem oder mehreren Rechtsvertretern der Organisation (wie in der rechtsgültigen Dokumentation über die Organisation angegeben) autorisiert werden und das Registrierungsformular muss von Hand geschriebene persönliche Unterschriften tragen. Im Bereich der Postzertifikate für Organisationen werden die Regeln zur Identifikation von Organisationen gemäss Verordnung des Eidgenössischen Finanzdepartements über elektronische Daten und Informationen (EIDI-V, SR 641.201.1) sowie der technischen und administrativen Vorschriften (TAV) der Eidgenössischen Steuerverwaltung (ESTV) zur EIDI-V (SR 641.201.11/Anhang) angewendet.

Der Rechtsvertreter muss einen Identitätsnachweis gemäss Kapitel 3.2.3 erbringen.

3.2.3 Authentisierung von natürlichen Personen

Einzelpersonen müssen eventuell die Verwendung von Namen in verschiedenen Teilen des DN autorisieren. Der Registrierungsvorgang jeder unter dieser CP/CPS operierenden Registrierungsstelle muss Massnahmen zur Feststellung der Identität solcher Einzelpersonen umfassen. Die in den Registrierungsformularen festgelegten Regeln können wie folgt zusammengefasst werden:

- Das Registrierungsformular muss von Hand geschriebene persönliche Originalunterschriften tragen. Pro Unterschrift sind hochwertige Kopien eines rechtsgültigen Lichtbildausweises dem Registrierungsformular beizulegen.
- Die im zur Identifikation vorgelegten Dokument enthaltenen Informationen müssen mit dem Namen und der Unterschrift auf dem Registrierungsformular übereinstimmen.
- Die Angaben im Antrag müssen mit dem/den in den zur Identifikation vorgelegten Dokumenten enthaltenen Vornamen und Nachnamen übereinstimmen.

Zusätzlich muss der Antragsteller – und zwar ausschliesslich der Antragsteller – entsprechend der folgenden zusätzlichen Regeln identifiziert werden:

- Der Antragsteller muss seine Identität mittels einer qualitativ einwandfreien, beglaubigten Kopie eines amtlichen, rechtsgültigen Lichtbildausweises belegen.

- Die Post legt fest, welche Lichtbildausweise und Beglaubigungen anerkannt werden.
- Das Feld /email= muss im Zuge des Registrierungsvorgangs überprüft werden. Der Antragsteller muss nachweisen, dass er Zugang zu der Mailbox hat und diese zum Empfang von Mails nutzen kann.

3.2.4 Nicht überprüfte Informationen

Es werden nur die in Kapitel 3.2.2 und 3.2.3 erforderlichen Informationen überprüft. Darüber hinaus werden keine Informationen überprüft.

3.2.5 Unterschriftsberechtigung

Der Antragssteller stellt eine aktuelle und gültige Dokumentation für den Organisations- oder Firmennamen bereit, der in das Zertifikat aufgenommen werden soll (z.B. Auszug aus dem Handelsregister, der aktuelle Informationen enthält, die nicht älter als 3 Monate sind). Die Schreibweise des Namens der Organisation oder Firma, die in das Zertifikat aufgenommen werden soll, muss exakt mit der Schreibweise in der bereitgestellten Dokumentation übereinstimmen.

Zudem muss die eingereichte Dokumentation belegen, dass mindestens diejenigen, welche die Unterschriften für die Organisation auf dem Registrierungsformular geleistet haben, durch die Organisation dazu befugt sind.

3.2.6 Kriterien für die gegenseitige Zertifizierung

SwissSign unterstützt eine gegenseitige Zertifizierung nicht.

3.3 Identifikation und Authentisierung für Anträge auf Zertifikatserneuerung

Die von dieser CA ausgestellten Zertifikate können nicht erneuert werden.

3.3.1 Identifikation und Authentisierung für Zertifikatserneuerung nach Ungültigerklärung

Die von dieser CA ausgestellten Zertifikate können nicht erneuert werden

3.4 Identifikation und Authentisierung für Anträge auf Ungültigerklärung

Zur Ungültigerklärung eines Zertifikats, das von dieser CA ausgestellt wurde, muss der Zertifikatsinhaber durch eines der folgenden Verfahren authentisiert werden:

- Nachweis des Besitzes des Private Key auf der RA Website;
- Revozierungspasswort (auf Hydalamdruck im Starter-Kit)
- mit einer persönlichen Unterschrift auf einem Formular zur Ungültigerklärung und unter Beilage einer hochwertigen Kopie eines rechtsgültigen Lichtbildausweises.

Das Verfahren zur Einreichung des Antrags auf Ungültigerklärung wird in Kapitel 4.9.3 beschrieben.

4 Betriebsanforderungen für den Zertifikatslebenszyklus

4.1 Zertifikatsantrag

4.1.1 Wer kann einen Zertifikatsantrag einreichen

Anträge können von natürlichen Personen und von Organisationen via bevollmächtigte natürliche Person eingereicht werden, die den im Registrierungsformular, der CP/CPS und den jeweils geltenden Allgemeinen Geschäftsbedingungen genannten Bestimmungen entsprechen.

4.1.2 Registrierungsverfahren

Der Antragssteller muss die Registrierungsformalitäten der Post befolgen. Das Zertifikat wird nur nach erfolgreichem Abschluss des Registrierungsverfahrens ausgestellt. Die grundlegenden Schritte zur Registrierung eines Zertifikats lauten:

- Die kompletten Registrierungsformulare wurden unterzeichnet und die Allgemeinen Geschäftsbedingungen wurden vom Antragssteller akzeptiert. Die Sicherheitshinweise wurden aktiv zur Kenntnis genommen. Aktiv bedeutet in diesem Fall, dass der Kunde eine entsprechende Checkbox aktivieren muss. Die Kenntnisnahme des CP/CPS wird ermöglicht, ist jedoch für das Registrierungsverfahren optional, da die wesentlichen Punkte in die AGB eingeflossen sind,
- ein von der Post anerkannter Identitätsnachweis ist vorhanden,
- alle Dokumente und Informationen werden von der RA der Post akzeptiert;
- und die RA der Post stellt ein SSCD bereit.

4.2 Bearbeitung des Zertifikatsantrags

4.2.1 Durchführung von Identifikation und Authentisierung

Die RA der Post identifiziert den Antragsteller anhand der vom Antragsteller zur Identifikation vorgelegten Dokumente, wie in Kapitel 3.2 festgelegt. Der Antragsteller muss die gesamte Dokumentation persönlich vorlegen.

4.2.2 Genehmigung oder Ablehnung von Zertifikatsanträgen

Die RA der Post genehmigt einen Zertifikatsantrag wenn alle folgenden Kriterien erfüllt sind:

- der Antragsteller hat die gesamte Dokumentation zur Identifizierung persönlich vorgelegt;
- die gesamte Dokumentation wurde empfangen und erfolgreich überprüft;
- die im Registrierungsformular enthaltenen Informationen werden als angemessen und vollständig eingestuft;
- die Überprüfung der Eindeutigkeit von Namen gemäss Kapitel 3.1.5 hat keine Kollisionen ergeben.

Wenn der Antragsteller eines der oben genannten Kriterien nicht erfüllt oder in anderer Weise die Bestimmungen dieses oder anderer relevanter Dokumente verletzt, muss die RA den Antrag ablehnen. Die Post behält sich das Recht vor, Zertifikatsanträge ohne Angabe von Gründen abzulehnen.

4.2.3 Dauer der Bearbeitung von Zertifikatsanträgen

Die Bearbeitung von Anträgen erfolgt in nützlicher Frist.

4.3 Ausstellung von Zertifikaten

4.3.1 Von der CA bei der Zertifikatsausstellung durchgeführte Schritte

Dieses Kapitel wird im CP/CPS der Root CA „SwissSign Platinum CP/CPS“ spezifiziert.

4.3.2 Benachrichtigung über die Zertifikatsausstellung

Der Antragsteller wird durch die Post RA über die Zertifikatsausstellung per E-Mail informiert.

4.4 Annahme von Zertifikaten

4.4.1 Als Annahme des Zertifikats geltende Handlungen

Der Zertifikatsinhaber kann seine Zertifikate über einen Link herunterladen, welchen er via E-Mail erhalten hat. Mit dem Download bestätigt er die Annahme der Zertifikate.

4.4.2 Veröffentlichung des Zertifikats durch die CA

Der Antragsteller erklärt sich damit einverstanden, dass die SwissSign AG unter Einhaltung geltender Vorschriften Informationen zum Zertifikatsstatus (CRL) veröffentlicht. Der Antragsteller entscheidet im Zuge des Registrierungsverfahrens, ob das Zertifikat im LDAP-directory veröffentlicht werden soll.

Die RA der Post kann jederzeit alle Zertifikate herunterladen, die aus dieser CA ausgestellt wurden. Diese Möglichkeit steht keinen weiteren Personen oder Organisationen zur Verfügung.

4.4.3 Benachrichtigung anderer Stellen durch die CA über die Zertifikatsausstellung

Der Prozess der Zertifikatsausstellung endet mit der Übermittlung des Zertifikats an die RA der Post. Eine weitere Benachrichtigung ist nicht vorgesehen.

4.5 Nutzung von Schlüsselpaaren und Zertifikaten

4.5.1 Nutzung von Private Keys und Zertifikaten durch Zertifikatsinhaber

Die Nutzung von Zertifikaten durch Zertifikatsinhaber muss den in den Ziffer 1.1.1 und 1.4.1 festgelegten Grundsätzen entsprechen.

4.5.2 Nutzung von Public Keys und Zertifikaten durch Zertifikatsprüfer

Die Zertifikatsprüfer haben sich an die in Ziffer 1.3.4 festgelegten Grundsätze zu halten.

4.6 Verlängerung von Zertifikaten (Certificate Renewal)

Die Verlängerung von Zertifikaten ist ein Vorgang, bei dem ein neues Zertifikat an einen Zertifikatsinhaber ausgestellt wird. Das Zertifikat enthält neue Gültigkeitsdaten, während die Informationen zu Subject und Schlüssel gleich bleiben.

Der Vorgang der Zertifikatsverlängerung wird nicht unterstützt.

4.7 Zertifikatserneuerung (Certificate Re-Key)

Die Zertifikatserneuerung ist ein Vorgang, bei dem der Zertifikatsinhaber automatisch ein neues Zertifikat erhält, wenn er den Besitz des Schlüssels für das alte Zertifikat nachweisen kann. Das so erstellte Zertifikat enthält neue Gültigkeitsdaten und ein neues Schlüsselpaar, während das Subject gleich bleibt.

Eine Zertifikatserneuerung wird nicht unterstützt.

4.8 Änderung von Zertifikaten

Die Änderung von Zertifikaten ist ein Vorgang, bei dem ein Zertifikatsinhaber ein Zertifikat mit geänderten Informationen zum Subject beantragt.

Eine Zertifikatsänderung wird nicht unterstützt. Die Post RA verfährt mit diesen Anträgen wie mit Anträgen auf eine Erstregistrierung.

4.9 Ungültigerklärung und Suspendierung von Zertifikaten

4.9.1 Voraussetzungen für die Ungültigerklärung

Die Zertifikatsinhaber können ihre Zertifikate jederzeit für ungültig erklären. Sie sind verpflichtet, unverzüglich die Ungültigkeit zu beantragen, wenn einer der folgenden Gründe vorliegt:

- bei Verlust oder Diebstahl der sicheren Signaturerstellungseinheit oder bei Verdacht auf Missbrauch derselben;
- bei Vermutung, dass ein Dritter Kenntnis des Sperrkennwortes erlangt haben könnte;
- bei Änderung von Angaben, welche in den Zertifikaten enthalten sind (z.B. E-Mailadresse, Name, Organisationsbezeichnung);
- sobald die sichere Signaturerstellungseinheit mit den darauf gespeicherten digitalen Schlüsseln nicht mehr benötigt wird.

Die CA ist befugt Zertifikate von sich aus für ungültig zu erklären, wenn sich herausstellt dass:

- diese unrechtmässig erlangt worden sind;
- keine Gewähr mehr dafür besteht, dass sie ausschliesslich dem Zertifikatsinhaber zugeordnet werden können (z.B. weil die dem Signaturzertifikat zugrunde liegenden Algorithmen gebrochen wurden);
- der Zertifikatsinhaber im Zahlungsverzug ist;
- das Vertragsverhältnis zwischen Zertifikatsinhaber und der Post endet;
- Angaben, welche in den Zertifikaten sind, geändert haben;
- die sichere Signaturerstellungseinheit des Zertifikatsinhabers verloren gegangen ist;
- das ausgestellte Zertifikat nicht den Bestimmungen und Bedingungen dieser CP/CPS entspricht;
- der Zertifikatsinhaber die vereinbarten Bedingungen und/oder andere geltende Gesetze, Regeln und Richtlinien nicht einhält.

4.9.2 Wer kann eine Ungültigerklärung beantragen

Die Post RA (siehe Ziff. 3.4) nimmt Anträge zur Ungültigerklärung von Zertifikaten von folgenden Parteien entgegen:

- dem Zertifikatsinhaber;
- einem autorisierten Vertreter des Unternehmens, das den Inhalt des Felds /O= im Zertifikat genehmigt hat;
- einem Schweizer Gericht.

4.9.3 Verfahren zur Beantragung einer Ungültigerklärung

Zur erfolgreichen Ungültigerklärung eines Zertifikats kann eines der folgenden Verfahren angewandt werden:

Der Besitzer des Private Key kann eine SSL-Sitzung mit starker Authentisierung nutzen, um das Zertifikat online für ungültig zu erklären.

Der Zertifikatsinhaber bekommt im Starter-Kit zu dem SSCD auch einen Hydalamdruck mit einem gesicherten Revozierungspasswort. Dieses Passwort kann auf der Post Webseite eingegeben werden, um die zugehörigen Zertifikate zu revozieren.

Der Zertifikatsinhaber kann unter Nutzung des Formulars zur Ungültigerklärung einen schriftlichen Antrag auf Ungültigerklärung einreichen. Um autorisiert zu sein, muss ein solcher Antrag die persönliche Unterschrift des ursprünglichen Antragstellers des Zertifikats tragen, mit einem Identitätsnachweis versehen sein (wie in Kapitel 3.2.3 beschrieben) und kann optional per Einschreiben versandt werden.

Im Falle eines Zertifikats für Organisationen oder eines Zertifikates mit Organisationsbezeichnung, kann auch ein autorisierter Vertreter der Organisation die Revokation mit einem Formular beantragen. Der Antrag muss einen Identitätsnachweis und einen Nachweis für die Authorisierung durch die Organisation enthalten.

Die offline durchgeführten Verfahren zur Ungültigerklärung dauern meist einige Tage länger als die online durchgeführten Ungültigerklärungen. Der Zertifikatsinhaber übernimmt die volle Verantwortung für jegliche Verzögerungen, die aus dem für die Ungültigerklärung gewählten Verfahren resultieren.

4.9.4 Frist für die Anträge auf Ungültigerklärung

Der Zertifikatsinhaber muss unverzüglich die Ungültigkeitserklärung verlangen wenn einer der Gründe aus Kapitel 4.9.1 zutrifft.

4.9.5 Frist für die Bearbeitung der Anträge auf Ungültigerklärung durch die CA

Die Frist für die Bearbeitung durch die CA wird im SwissSign Platinum CP/CPS beschrieben.

Die Post RA garantiert, dass korrekt eingereichte Anträge auf Ungültigerklärung innert eines Arbeitstages nach Antragseingang an die CA weitergemeldet werden.

4.9.6 Prüfpflichten der Zertifikatsprüfer in Bezug auf die Ungültigerklärung

Dieses Kapitel wird im SwissSign Platinum CP/CPS beschrieben.

4.9.7 Häufigkeit der CRL-Ausstellung

Dieses Kapitel wird im SwissSign Platinum CP/CPS beschrieben.

4.9.8 Maximale Verzögerung für CRLs

Dieses Kapitel wird im SwissSign Platinum CP/CPS beschrieben.

4.9.9 Option zur Online-Überprüfung von Ungültigerklärungen/Status

Dieses Kapitel wird im SwissSign Platinum CP/CPS beschrieben.

4.9.10 Anforderungen für die Online-Überprüfung von Ungültigerklärungen

Zertifikatsprüfer sind verpflichtet, die von dieser CA ausgegeben Zertifikate zu überprüfen. Diese Prüfung kann mittels dem OCSP-Protokoll zur Online-Überprüfung von Ungültigerklärungen erfolgen. Die URL des OCSP Responders ist in jedem der Swiss Post Platinum Zertifikate gespeichert (Feld «Authority Info Access»).

4.9.11 Weitere verfügbare Optionen der Ungültigkeitsbekanntmachung

Dieses Kapitel wird im SwissSign Platinum CP/CPS beschrieben.

4.9.12 Besondere Anforderungen bei einer Verletzung des Schlüssels

Wenn ein Zertifikatsinhaber weiss oder vermutet, dass die Integrität des Private Key seines Zertifikats verletzt wurde, so muss er:

- die Nutzung des Zertifikats sofort einstellen;
- sofort die Ungültigerklärung des Zertifikats veranlassen;
- das Zertifikat von allen Geräten und Systemen löschen;
- alle Zertifikatsprüfer informieren, die sich evtl. auf dieses Zertifikat verlassen.

Die Verletzung des Private Key kann Auswirkungen auf die durch diesen Schlüssel geschützten Informationen haben. Der Zertifikatsinhaber muss entscheiden, wie er mit den betroffenen Informationen verfahren will, bevor er den verletzten Schlüssel löscht. Er ist befugt, den Private Key zur Entschlüsselung bereits verschlüsselter Daten zu verwenden.

4.9.13 Voraussetzungen für die Suspendierung

Eine Suspendierung von Zertifikaten, welche von dieser CA ausgegeben werden, ist nicht möglich.

4.10 Dienste zum Zertifikatsstatus

Dieses Kapitel wird im SwissSign Platinum CP/CPS beschrieben.

4.11 Ende der Zertifikatsnutzung

Das Ende der Zertifikatsnutzung tritt ein, wenn:

- ein Zertifikat des Zertifikatssets für ungültig erklärt wurde;
- die Gültigkeitsdauer eines Zertifikates abgelaufen ist.

4.12 Hinterlegung und Wiederherstellung von Schlüsseln

Nur die Schlüssel der Verschlüsselungszertifikate können hinterlegt und wiederhergestellt werden, falls dies durch den Antragssteller bei der Registration gewünscht wurde. Für andere Schlüssel wird keine Hinterlegung oder Wiederherstellung angeboten.

5 Einrichtung, Verwaltung und Betriebskontrollen

5.1 Physische Kontrollen

Die RA Post Server befinden sich in einem nach allgemein anerkannten Sicherheitsstandards geschützten und gesicherten Rechenzentrum.

5.1.1 Lage und Beschaffenheit der Standorte

Das Rechenzentrum der RA Post befindet sich im Grossraum Luzern in der Schweiz.

5.1.2 Physischer Zugang

Der physische Zugang zum Rechenzentrum ist auf Systemadministratoren und autorisiertes Personal beschränkt. Der Zutritt ist nur mittels eines elektronischen Schlüssels möglich. Das Rechenzentrum ist videoüberwacht. Die Zutritte werden aufgezeichnet.

5.1.3 Stromversorgung und Klimatisierung

Das Rechenzentrum ist klimatisiert, um eine optimale Umgebung für das System nach allgemein anerkannten Verfahrensweisen zu schaffen. Die Stromversorgung wird mit einer unterbrechungsfreien, batteriegestützten Stromversorgung ergänzt.

5.1.4 Risiko eines Wassereintruchs

Das Rechenzentrum ist mit Wassermeldern ausgestattet. Ein angemessenes Warnsystem ist vorhanden. Das Rechenzentrum befindet sich in einem Gebiet ohne besondere Überschwemmungsrisiken. Das Rechenzentrum befindet sich in einem oberen Stockwerk.

5.1.5 Brandschutz

Das Rechenzentrum ist mit einem angemessenen Brandmeldesystem ausgerüstet.

5.1.6 Medienspeicherung

Die Entsorgung von Speichermedien wird durch einen darauf spezialisierten Drittanbieter übernommen.

5.1.7 Abfallentsorgung

Fallen beim Betrieb der RA Abfälle an, werden diese von einem spezialisierten Drittanbieter kontrolliert entsorgt und vernichtet.

5.1.8 Entfernt gelagerte Backups

Die Backups der RA Post werden in einem vom Rechenzentrum räumlich getrennten Tresor aufbewahrt, zu welchem

nur autorisierte Personen Zugang haben.

5.2 Verfahrenskontrollen

5.2.1 Vertrauenswürdige Rollen

Um eine Aufteilung der Pflichten zu gewährleisten, wird die RA Post von zwei getrennten Autorisierungsgruppen betrieben. Dabei handelt es sich um eine Gruppe Systemadministrator (SA, Access) und eine Gruppe Betrieb (RAO, Operations). Jeder Mitarbeiter kann nur einer dieser Autorisierungsgruppen angehören.

5.2.1.1 Zugang

Systemadministratoren (SA) haben die volle Kontrolle über das Netzwerk, die Hardware, das Betriebssystem und die Anwendungssoftware, welche zusammen die RA Post bilden. Sie haben keinen Zugriff auf die Private-Keys, welche die Kommunikation der RA Post mit der CA schützen.

Der SA ist autorisiert, die Systeme der RA Post zu installieren, konfigurieren und zu verwalten. Der SA ist zur Durchführung von Backups und Wiederherstellungen des Systems autorisiert.

5.2.1.2 Betrieb

Die RA Operatoren (Registration Authority Operators – RAO) können eine Unterauswahl an Zertifikaten und Anträgen, verwalten. Der RAO kann die Definition der RA nicht ändern. Der RAO ist für den täglichen Betrieb der RA Post verantwortlich.

5.2.2 Anzahl der pro Aufgabe erforderlichen Personen

Der Betrieb der RA Post ist rollenbasiert und erfordert daher mindestens:

- Zugang: mindestens 2 Mitarbeiter für Aufgaben in der Konfiguration des Netzwerkzugriffs, der Systemadministration sowie der Wartung und Verwaltung der RA Post.
- Betrieb: mindestens 2 Mitarbeiter für den Betrieb von RA Post.

5.2.3 Identifikation und Authentisierung für die einzelnen Rollen

Die Identifikation und Autorisierung für die Rolle Zugang erfolgt durch Anmeldung mit Benutzernamen und Passwort. Die Identifikation und Autorisierung für die Rolle RAO erfolgt durch Verwendung von SwissSign Zertifikaten.

5.2.4 Rollen mit getrennten Pflichten

Um eine strikte Trennung der Pflichten, wie in Abschnitt 5.2.1 beschrieben, zu gewährleisten, müssen die Rollen in Bezug auf Zugang und Betrieb an verschiedene Personen vergeben werden.

5.3 Personalkontrollen

5.3.1 Qualifikation, Erfahrung, Überprüfungsanforderungen

Um die Rolle «Zugang» zugewiesen zu bekommen, muss ein Mitarbeiter über Fachkenntnisse in Bezug auf TCP/IP-Netzwerke, Unix-Betriebssysteme und Technologie, Konzepte und Anwendungen der PKI verfügen.

Um die Rolle «Betrieb» zugewiesen zu bekommen, muss ein Mitarbeiter über Fachkenntnisse in Bezug auf Technologie und Anwendungen, welche die PKI nutzen, verfügen. Er muss auch über gute Fähigkeiten im Umgang

mit anderen Menschen und ein umfassendes Verständnis der PKI-Prozesse verfügen.

Vor Aufnahme ihrer Tätigkeit bei der RA Post müssen sämtliche Mitarbeiter eine Vereinbarung zur Vertraulichkeit und Geheimhaltung unterzeichnen. Zudem müssen diese Mitarbeiter im Bereich Sicherheit, Sicherheitstechnologie und Sicherheitsmethodik adäquat ausgebildet sein.

5.3.2 Verfahren zur Überprüfung des Hintergrunds

Die RA Post stellt keine Personen ein, von denen der RA Post bekannt ist, dass sie wegen eines schwerwiegenden Verbrechens oder Vergehens verurteilt wurden, welche ihre Eignung für die jeweilige Position beeinträchtigen könnte. Bei Neu- oder Wiederanstellungen werden Strafregisterauszüge verlangt.

5.3.3 Schulungsanforderungen

Werden Mängel bei erforderlichen Fachkenntnissen festgestellt, werden diese durch geeignete Schulungsmassnahmen behoben. Diese Schulungsmassnahmen werden durch die Leitung RA Post bestimmt.

5.3.4 Häufigkeit der Fortbildung und Anforderungen

Die Fortbildung der Mitarbeiter erfolgt je nach Bedarf, abhängig von den Anforderungen des Unternehmens oder der Einzelperson.

5.3.5 Häufigkeit und Abfolge von Stellenwechseln

Ein Stellenwechsel der Mitarbeiter erfolgt je nach Bedarf, abhängig von den Anforderungen des Unternehmens oder auf Antrag der Einzelperson.

5.3.6 Strafen für nicht autorisiertes Vorgehen

Die RA Post behält sich das Recht vor, ein nicht autorisiertes Vorgehen im vollen Umfang geltender Schweizer Gesetze zu verfolgen.

5.3.7 Anforderungen für unabhängige Vertragsnehmer

Die RA Post garantiert, dass allfällige Dritte, welche sie bezieht, sorgfältig ausgewählt werden. Die Dritten werden auf Geheimhaltung verpflichtet.

5.3.8 Dem Personal bereitgestellte Dokumentation

Die RA Post stellt ihren Mitarbeitern die für die Ausübung ihrer Tätigkeit notwendigen Dokumentationen und Arbeitsanweisungen zur Verfügung.

5.4 Verfahren zur Audit-Protokollierung

Die RA Post ist so konzipiert, dass sie alle Vorgänge rund um eine Zertifikatsausstellung und Zertifikatsrevozierung protokolliert.

5.4.1 Art der aufgezeichneten Vorgänge

Die folgenden Vorgänge werden aufgezeichnet:

- neue Zertifikatsanträge
- Bewilligung von Anträgen durch den RAO

Classification: C1 (öffentlich)
Applicability: Global
Owner: CEO
Issue Date: April 28th, 2008
Version: 1.1.1
Storage: Swiss-Post-Platinum-CP-CPS-V0114.doc

- abgelehnte Zertifikatsanträge
- Ungültigerklärung von Zertifikaten
- Anmeldung bei Benutzerkonten
- Ablauf von Zertifikaten
- Download/Installation von Zertifikaten

Die oben stehende Liste ist nicht abschliessend und ausserdem auf Vorgänge beschränkt, die in direktem Zusammenhang mit der Zertifikatsverwaltung stehen. Insbesondere umfasst sie keine technischen Vorgänge, die an einer anderen Stelle protokolliert werden.

5.4.2 Häufigkeit der Protokollverarbeitung

Die Protokolle werden in regelmässigen Abständen und bei Verdachtsmomenten auditiert.

5.4.3 Archivierungsdauer für das Auditprotokoll

Die Protokoll Daten in der RA Post Datenbank werden nie gelöscht.

5.4.4 Schutz des Auditprotokolls

Ein Lesezugriff wird für Mitarbeiter gewährt, die diesen Zugang im Zuge Ihrer Pflichten benötigen. Die folgenden Rollen können diesen Zugang erhalten:

- RAO
- SA

Das Protokollbuch wird in der Datenbank gespeichert.

5.4.5 Verfahren zum Backup des Auditprotokolls

Das Protokollbuch ist ein fester Bestandteil der RA Post Datenbank und unterliegt daher dem täglichen Backup. Nur Mitarbeiter mit der Rolle SA, sowie autorisierte Personen haben Zugang zu den Backupmedien.

5.4.6 Auditerfassungssystem (intern bzw. extern)

Das Auditprotokoll oder Protokollbuch ist ein fester Bestandteil der RA Post Software.

5.4.7 Benachrichtigung des den Vorgang verursachenden Inhabers

Es ist nicht vorgesehen, dass der Zertifikatsinhaber über Protokolleinträge informiert wird.

5.4.8 Bewertung von Sicherheitslücken

Die RA Post behält sich das Recht vor, die Schweizer Behörden oder die SwissSign AG über Versuche zu informieren einen nicht autorisierten Zugang zu erlangen.

5.5 Archivierung von Aufzeichnungen

5.5.1 Art der archivierten Aufzeichnungen

Die zur Antragsstellung eingereichten Dokumente werden elektronisch archiviert.

5.5.2 Archivierungsdauer

Archivierte Daten werden für einen Zeitraum von mindestens 11 Jahren nach der Beendigung der Zertifikatsnutzung aufbewahrt, wie in Kapitel 4.11 angegeben.

5.5.3 Schutz des Archivs

Der Schutz des Archivs besteht in folgenden Massnahmen:

- Die archivierten Daten sind nur Mitarbeitern der RA Post in der Rolle SA, oder autorisierten Personen zugänglich.
- Nachvollziehbarkeit vor Änderungen: Die Registrierungsdaten von Zertifikatsnutzern werden digital signiert.

5.5.4 Verfahren zum Backup des Archivs

Die archivierten Daten werden bei der RA Post in einem Tresor gelagert.

5.5.5 Anforderungen für die Datierung der Aufzeichnungen

Alle in der Datenbank sowie in den Protokolldateien enthaltenen Daten werden mit der Systemzeit des Systems zum Zeitpunkt der Aufzeichnung des Vorgangs datiert.

Die Systemzeit aller Server wird mittels einer Zeitquelle im Internet synchronisiert.

Die eingescannten Registrierungsdaten erhalten mit der digitalen Signatur einen Zeitstempel.

5.5.6 Archiverfassungssystem (intern bzw. extern)

Die RA Post verwendet ein internes Archiverfassungssystem.

5.5.7 Verfahren zur Erlangung und Überprüfung archivierter Daten

Auf Verlangen der berechtigten Person oder auf gerichtliche Anordnung wird eine hochwertige Kopie der archivierten Registrierungsdaten erstellt und zur Verfügung gestellt. Diese Kopie wird nach der Rückgabe zerstört. Dieser Vorgang wird protokolliert. Für diese Arbeiten kann eine Gebühr erhoben werden.

5.6 Auswechseln der Schlüssel

Dieses Kapitel wird im SwissSign Platinum CP/CPS beschrieben.

5.7 Verletzungen und Wiederherstellung im Notfall

5.7.1 Verfahren zur Handhabung von Zwischenfällen und Verletzungen

RA Post wendet für die Handhabung von Zwischenfällen folgendes Modell an:

Classification:	C1 (öffentlich)
Applicability:	Global
Owner:	CEO
Issue Date:	April 28th, 2008
Version:	1.1.1
Storage:	Swiss-Post-Platinum-CP-CPS-V0114.doc

- Eine Service-Stelle nimmt alle eingehenden Service-Anrufe entgegen und stuft sie nach ihrer Bedeutung geordnet ein.
- Die Leitung RA Post ist dafür besorgt den Normalzustand so schnell wie möglich wieder herzustellen.

Wiederholt auftretende Zwischenfälle oder Zwischenfälle mit weit reichenden Folgen werden in den Problemmanagementprozess übernommen. Dieser soll die grundlegende Ursache des Problems bestimmen und weitere Probleme vermeiden.

5.7.2 Beschädigte Rechenressourcen, Software und/oder Daten

Die Serversysteme der RA Post sind mit gewissen redundanten Bauteilen gegen Ausfall geschützt. Die Serversysteme selber sind nicht redundant ausgelegt.

5.7.3 Verfahren bei kompromittierten privaten Schlüsseln

Dieses Kapitel wird im SwissSign Platinum CP/CPS beschrieben.

5.7.4 Geschäftskontinuität nach Notfällen

Bei Notfällen unternimmt die Leitung der RA Post alles, um die Geschäftskontinuität so schnell als möglich sicherzustellen.

5.8 Beendigung der CA oder RA

Dieses Kapitel wird im SwissSign Platinum CP/CPS beschrieben.

Die Information der Kunden und der Registrierungsstellen erfolgt, nach Absprache mit der Betreiberin der CA, per signiertes E-Mail durch die Schweizerische Post. Sollte die Benachrichtigung per E-Mail nicht möglich sein, so erfolgt die Information schriftlich. Die Information erläutert den Grund der Beendigung und zeigt das weitere Vorgehensszenario auf. Die Information hat so zu erfolgen, dass, sofern es die Umstände zulassen, allen involvierten Parteien eine angemessene Frist für die Umstellung auf die neue Gegebenheit eingeräumt wird.

6 Technische Sicherheitskontrollen

Abgesehen von den nachfolgenden Bestimmungen sind alle technischen Sicherheitskontrollen betreffend der Platin CAs im SwissSign Platinum CP/CPS beschrieben.

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

Die Schlüsselpaare der Zertifikatsinhaber für Zertifikate werden auf genehmigten Signaturerstellungseinheiten (z.B. Smart Card, USB Token) durch die Post erzeugt.

Die Schlüsselpaare der Zertifikatsinhaber für Verschlüsselungszertifikate können auf Wunsch des Antragsstellers auch ausserhalb des SSCD in einer geschützten Umgebung durch die Post erzeugt werden.

6.1.2 Bereitstellung des Private Key an den Zertifikatsinhaber

Die auf einem genehmigten SSCD erzeugten Private Keys werden durch die Post bereitgestellt und herausgegeben.

Der Private Key des Verschlüsselungszertifikats, welcher ausserhalb des SSCD gemäss Kapitel 6.1.1 erzeugt wurde, wird verschlüsselt zum Herunterladen von der Post Webseite bereitgestellt.

6.1.3 Bereitstellung des Public Key an den Zertifikatsaussteller

Der Public Key wird nach dem Erzeugen des Schlüsselpaares gespeichert und in der DB der Post RA hinterlegt. Die Post RA übergibt den Public Key als Teil des nach PKCS#10 formatierten Antrag auf Zertifikatssignierung über einen sicheren SSL-verschlüsselten Kommunikationskanal an die signierende CA.

6.1.4 Bereitstellung des Public Key der CA an die Zertifikatsprüfer

Die Zertifikatsprüfer können das Zertifikat der ausstellenden CA unter Verwendung des PKCS#7-Formats von der SwissSign Website herunterladen.

Wenn ein Zertifikatsprüfer das Zertifikat erhält, ist der Public Key der ausstellenden CA enthalten. Ebenfalls enthalten ist die vollständige Kette der Zertifikate der hierarchischen SwissSign PKI einschliesslich aller Public Keys, die zu der Vertrauenskette gehören.

6.1.5 Schlüssellänge

Alle Zertifikatsinhaber verwenden 2048 Bit RSA Schlüssel.

6.1.6 Erzeugung und Qualitätsprüfung von Public Key-Parametern

Die Schlüssel werden durch die Post generiert und daher werden auch die Parameter durch die Post gesetzt.

6.1.7 Verwendungszweck der Schlüssel (gemäss Feld «KeyUsage X.509 v3»)

Zertifikatsinhaber können Zertifikate erhalten, in denen eines oder mehrere der folgenden Bits im Feld «KeyUsage»

Classification:	C1 (offentlich)
Applicability:	Global
Owner:	CEO
Issue Date:	April 28th, 2008
Version:	1.1.1
Storage:	Swiss-Post-Platinum-CP-CPS-V0114.doc

gesetzt sind:

digitalSignature

nonRepudiation

keyAgreement

dataEncipherment

keyEncipherment

Erweiterte Geltungsbereiche der Zertifikate:

secureEmail

clientAuthentication

Microsoft Smart Card Logon.

Microsoft Encrypted File System

6.2 Schutz der Private Keys und Kontrolle beim Erstellen von Verschlüsselungsmodulen

6.2.1 Standards und Kontrollen für Verschlüsselungsmodule

Die folgende Liste zeigt, wie die Anforderungen für die verschiedenen Nutzer der SSCD implementiert werden:

Schlüssel der Zertifikatsinhaber	Diese Schlüssel werden auf einer SSCD erzeugt und gespeichert, welche die EAL 4+-Zertifizierung erfüllt. Alternativ können die Schlüssel für die Verschlüsselung auch ausserhalb erzeugt werden gemäss Kapitel 6.1.1.
----------------------------------	---

6.2.2 Kontrolle des Private Key durch mehrere Personen (M of N)

Die folgende Liste zeigt, wie Kontrollen durch mehrere Personen implementiert werden:

Schlüssel der Zertifikatsinhaber	Der Registrierungsprozess stellt sicher, dass der Zertifikatsinhaber die einzige Instanz ist, die Zugang zu den Schlüsseln auf der SSCD des Zertifikatsinhabers hat. Die hinterlegten Schlüssel der Verschlüsselung werden über einen MofN Mechanismus geschützt.
----------------------------------	---

6.2.3 Hinterlegung des Private Key

Die folgende Liste zeigt, wie die Hinterlegung des Private Key implementiert wird:

Schlüssel der Zertifikatsinhaber	Eine Hinterlegung des Private Key wird nur für die Schlüssel der Verschlüsselung angeboten. Der Zertifikatsinhaber kann das Angebot aber auch ausschlagen. Der Private Key wird doppelt hinterlegt, einmal verschlüsselt mit einem Passwort welches durch den Zertifikatsinhaber gewählt wurde und einmal verschlüsselt mit einem Public Key, wobei der zugehörige Private Key MofN geschützt ist.
----------------------------------	--

6.2.4 Backup des Private Key

Die folgende Liste zeigt, wie der Backup des Private Key implementiert wird:

Schlüssel der Zertifikatsinhaber	Die Post RA bietet einen Backup des Private Key für das Schlüsselpaar der Verschlüsselung. Ein Schlüsselpaar wird gespeichert und ist durch ein vom Zertifikatsinhaber gewähltes Passwort aus mindestens 8 (empfohlen 16) Zeichen geschützt. Alle anderen Schlüssel werden auf der SSCD erzeugt und können nicht im Backup übernommen werden.
----------------------------------	---

6.2.5 Archivierung des Private Key

Die folgende Liste zeigt, wie die Archivierung des Private Key implementiert wird:

Schlüssel der Zertifikatsinhaber	Die Post RA bietet den Zertifikatsinhabern die Option zum Download ihrer Private Keys für die Verschlüsselung in Form einer PKCS#12-Datei. Die Zertifikatsinhaber können diese Datei archivieren. Diese Schlüsselpaare werden auch in der Post RA gespeichert, die im Backup übernommen und archiviert wird. Alle anderen Schlüssel werden auf der SSCD erzeugt und können nicht extrahiert werden.
----------------------------------	---

6.2.6 Übertragung des Private Key an und von Verschlüsselungsmodule(n)

Die folgende Liste zeigt, wie die Übertragung des Private Key implementiert wird:

Schlüssel der Zertifikatsinhaber	Auf der SSCD erzeugte Schlüssel von Zertifikatsinhabern können nicht geklont werden. Die Private Keys für die Verschlüsselung können mit Hilfe der üblichen Verfahren für Backup und Wiederherstellung geklont werden. Die Kontrollen für diese Prozesse sind in Kapitel 6.2.4 «Backup des Private Key» beschrieben.
----------------------------------	--

6.2.7 Speicherung des Private Key auf Verschlüsselungsmodulen

Die folgende Liste zeigt, wie Private Keys auf Verschlüsselungsmodulen gespeichert werden:

Schlüssel der Zertifikatsinhaber	Die Schlüssel der Zertifikatsinhaber werden auf Verschlüsselungsmodulen gespeichert, so dass sie nur bei ordnungsgemässer Aktivierung genutzt werden können.
----------------------------------	--

6.2.8 Verfahren zur Aktivierung des Private Key

Die folgende Liste zeigt, wie Private Keys aktiviert werden:

Schlüssel der Zertifikatsinhaber	Die Schlüssel der Zertifikatsinhaber werden mit einer Token PIN aktiviert gemäss EAL 4+ Zertifizierung.
----------------------------------	---

6.2.9 Verfahren zur Deaktivierung des Private Key

Die folgende Liste zeigt, wie Private Keys deaktiviert werden:

Schlüssel der Zertifikatsinhaber	Die Schlüssel der Zertifikatsinhaber werden durch Entfernen der SSCD vom Computer oder durch Beenden der Anwendung, die Zugang zu der SSCD hatte, deaktiviert.
----------------------------------	--

6.2.10 Verfahren zur Vernichtung des Private Key

Die folgende Liste zeigt, wie Private Keys vernichtet werden:

Schlüssel der Zertifikatsinhaber	Die Schlüssel der Zertifikatsinhaber können nur durch Vernichtung der SSCD vernichtet werden. Im Falle des Schlüsselpaars der Verschlüsselung ist eine Vernichtung nur dann möglich, wenn das Schlüsselpaar nie im Post RA Backup übernommen wurde.
----------------------------------	---

6.2.11 Einstufung der Verschlüsselungsmodule

Die Mindeststandards für Verschlüsselungsmodule sind in Kapitel 6.2.1 festgelegt.

6.3 Weitere Aspekte der Verwaltung von Schlüsselpaaren

6.3.1 Archivierung des Public Key

Dieses Kapitel wird im SwissSign Platinum CP/CPS behandelt.

6.3.2 Nutzungszeiträume von Zertifikaten und Schlüsselpaaren

Die Nutzungszeiträume für Zertifikate welche unter dieser CA ausgegeben werden lauten wie folgt:

- Zertifikate von ausstellenden CAs haben eine maximale Nutzungsdauer von 15 Jahren.
- Die Verlängerung von CA Zertifikaten wird manuell durchgeführt und ist danach höchstens zwei Drittel des Nutzungszeitraumes des Zertifikates.
- Zertifikate der Zertifikatsinhaber können eine Nutzungsdauer von bis zum Maximum der verbleibenden Nutzungsdauer des Zertifikates der ausstellenden CA minus 10 Tage haben.

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation von Aktivierungsdaten

Zum Schutz von Private Keys von SSCD verwendete Aktivierungsdaten werden gemäss den Anforderungen dieser CP/CPS erzeugt. Sie müssen:

- vom Zertifikatsinhaber erzeugt und nur diesem bekannt sein;
- aus mindestens sechs Zeichen bestehen;
- alphabetische und numerische Zeichen umfassen;
- nicht mehrmals wiederholt dasselbe Zeichen enthalten;
- keine Teile des Benutzernamens oder andere erschliessbare Wörter enthalten.

6.4.2 Schutz der Aktivierungsdaten

Die Zertifikatsinhaber sind verpflichtet, die Aktivierungsdaten stets geheim zu halten.

6.4.3 Weitere Aspekte der Aktivierungsdaten

Nicht anwendbar.

6.5 Sicherheitskontrollen der Computer

Dieses Kapitel wird im CP/CPS der Root CA „SwissSign Platinum CP/CPS“ spezifiziert.

Die Server der RA Post sind durch Firewalls geschützt. Der SA Zugang zum System erfolgt ausschliesslich über sichere Protokolle.

6.5.1 Spezifische technische Anforderungen für die Sicherheit der Computer

Die RA Post setzt ein in Schichten aufgeteiltes Sicherheitskonzept ein, um die Sicherheit und Integrität der zur

Ausführung der RA Post Software verwendeten Computer zu gewährleisten. Die folgenden Kontrollen stellen die Sicherheit der von RA Post betriebenen Computersysteme sicher:

- es werden nur Software-Pakete von vertrauenswürdigen Softwarearchiven installiert;
- minimale Netzwerkkonnektivität;
- Authentisierung und Autorisation für alle Funktionen;
- proaktives Patchmanagement.

6.6 Technische Kontrollen zum Lebenszyklus

Dieses Kapitel wird im CP/CPS der Root CA „SwissSign Platinum CP/CPS“ spezifiziert.

6.6.1 Systementwicklungssteuerung

Um die Qualität und Verfügbarkeit der RA Post-Software sicherzustellen werden folgende Grundregeln eingehalten:

- Vom Softwarearchiv wird regelmässig ein Backup erstellt.
- Eine Kontrolle des Software-Lebenszyklus basierend auf getrennten Umgebungen für Entwicklung, Test und Produktion ist vorhanden. Die Software-Lebenszykluskontrolle stellt sicher, dass die Kontrollen und Checkpoints im Unternehmen eingehalten werden.
- Interne Richtlinien zur Softwareentwicklung enthalten Standards und Grundsätze für die Software-Entwicklung.

6.6.2 Kontrollen zum Sicherheitsmanagement

Eine Überwachung stellt sicher, dass die Systeme und Netzwerke in Übereinstimmung mit der angegebenen Sicherheitspolitik betrieben werden. Alle Prozesse werden gemäss geltender Gesetze und Vorschriften protokolliert.

6.6.3 Sicherheitskontrollen zum Lebenszyklus

Die Entwicklung der Softwaresysteme entspricht den in den internen Richtlinien zur Softwareentwicklung angegebenen Prinzipien. Diese Richtlinien sind Teil eines Sicherheitsmanagementprozesses, der alle den Lebenszyklus betreffenden Sicherheitskontrollen abdeckt.

6.7 Sicherheitskontrollen des Netzwerks

Dieses Kapitel wird im CP/CPS der Root CA „SwissSign Platinum CP/CPS“ spezifiziert.

6.8 Datierung

Dieses Kapitel wird im CP/CPS der Root CA „SwissSign Platinum CP/CPS“ spezifiziert.

7 Zertifikats-, CRL- und OCSP-Profile

Abgesehen von den nachfolgenden Bestimmungen sind alle relevanten Regeln zu Zertifikats-, CRL-, und OCSP-Profile dieser CA im "SwissSign Platinum CP/CPS" beschrieben.

7.1 Zertifikatsprofil

Die „Swiss Post Platinum CA“ stellt in Übereinstimmung mit PKIX Zertifikate nach X.509 Version 3 aus. Diese Zertifikate sind wie folgt aufgebaut:

Zertifikatsfeld	Wert	Anmerkung
Version	X.509 Version 3	See Chapter 7.1.1
Serial number	Unique number	Will be used in CRL
Signature algorithm identifier	OID	See Chapter 7.1.3
Validity period	Start date, expiration date	
Subject Public Key Info	Public Key algorithm, Subject Public Key	See Chapter 7.1.3
Extensions	X509V3 Extensions	See Chapter 7.1.2
Signature	Certificate Signature	

7.1.1 Zertifikatserweiterungen

7.1.1.1 Erweiterungen des Swiss Post Platinum CA Zertifikats

Extension Attribute	Values	Comment
Subject	/CN=Swiss Post Platinum CA – G2 /O=SwissSign AG/C=CH	
Issuer Name	/CN=Swiss Platinum CA - G2 /O=SwissSign AG/C=CH	
Key Usage	Certificate Sign, CRL Sign	Critical extension
Basic Constraints	CA: TRUE, pathlen: 0	Critical extension
Subject Key Identifier	<key identifier of this CA's public key>	See Chapter 7.1.3
Authority Key Identifier	keyid: <key identifier of the issuing CA's public key>	See Chapter 7.1.3
CRL Distribution Points		URLs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy: 2.16.756.1.89.1.1.1.4.3 CPS: http://repository.swissign.com/Swiss-Post-Platinum-CP-CPS-R3.pdf	

7.1.1.2 Erweiterungen des Swiss Post Platinum Authentisierungszertifikats für natürliche Personen

Erweiterungsattribut	Werte	Anmerkung
Subject	Daten des Antragsstellers	Siehe Definition in Kapitel 1.6

Erweiterungsattribut	Werte	Anmerkung
Issuer Name	/CN=Swiss Post Platinum CA – G2 /O=SwissSign AG/C=CH	
Authority Key Identifier	keyid: <key identifier of the issuing CA's public key>	Siehe Kapitel 7.1.3
CRL Distribution Points		URIs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy: 2.16.756.1.89.1.1.1.4.3 CPS: http://repository.swissign.com/Swiss-Post-Platinum-CP-CPS-R3.pdf	QCP public + SSCD
Authority Information Access		URI to OCSP responder and optional URI to CA issuer certificate
Subject Alternative Name		Alternative name of the subscriber: email address
Key Usage	digitalSignature, keyAgreement	Critical extension
Extended Key Usage		Optional Siehe Kapitel 6.1.7 für mögliche Werte
NsComment		Optional
Microsoft Certificate Template	(OID 1.3.6.1.4.1.311.20.2)	Optional

7.1.1.3 Erweiterungen des Swiss Post Platinum Zertifikats für natürliche Personen

Erweiterungsattribut	Werte	Anmerkung
Subject	Daten des Antragsstellers	Siehe Definition in Kapitel 1.6
Issuer Name	/CN=Swiss Post Platinum CA – G2 /O=SwissSign AG/C=CH	
Authority Key Identifier	keyid: <key identifier of the issuing CA's public key>	Siehe Kapitel 7.1.3
CRL Distribution Points		URIs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy: 2.16.756.1.89.1.1.1.4.3 CPS: http://repository.swissign.com/Swiss-Post-Platinum-CP-CPS-R3.pdf	QCP public + SSCD
Authority Information Access		URI to OCSP responder and optional URI to CA issuer certificate
Subject Alternative Name		Alternative name of the subscriber: email address
Key Usage	nonRepudiation	Critical extension
Extended Key Usage		Optional Siehe Kapitel 6.1.7 für mögliche Werte
NsComment		Optional
Microsoft Certificate Template	(OID 1.3.6.1.4.1.311.20.2)	Optional

7.1.1.4 Erweiterungen des Swiss Post Platinum Verschlüsselungszertifikats für natürliche Personen

Erweiterungsattribut	Werte	Anmerkung
Subject	Daten des Antragsstellers	Siehe Definition in Kapitel 1.6
Issuer Name	/CN=Swiss Post Platinum CA – G2 /O=SwissSign AG/C=CH	
Authority Key Identifier	keyid: <key identifier of the issuing CA's public key>	Siehe Kapitel 7.1.3
CRL Distribution Points		URIs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy: 2.16.756.1.89.1.1.1.4.3 CPS: http://repository.swissign.com/Swiss-Post-Platinum-CP-CPS-R3.pdf	QCP public
Authority Information Access		URI to OCSP responder and optional URI to CA issuer certificate
Subject Alternative Name		Alternative name of the subscriber: email address
Key Usage	dataEncipherment, keyEncipherment	Critical extension
Extended Key Usage		Optional Siehe Kapitel 6.1.7 für mögliche Werte
NsComment		Optional
Microsoft Certificate Template	(OID 1.3.6.1.4.1.311.20.2)	Optional

7.1.1.5 Erweiterungen des Swiss Post Platinum Authentisierungszertifikats für Organisationen

Erweiterungsattribut	Werte	Anmerkung
Subject	Daten des Antragsstellers	Siehe Definition in Kapitel 1.6
Issuer Name	/CN=Swiss Post Platinum CA – G2 /O=SwissSign AG/C=CH	
Authority Key Identifier	keyid: <key identifier of the issuing CA's public key>	Siehe Kapitel 7.1.3
CRL Distribution Points		URIs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy: 2.16.756.1.89.1.1.1.4.3 CPS: http://repository.swissign.com/Swiss-Post-Platinum-CP-CPS-R3.pdf	QCP public + SSCD
Authority Information Access		URI to OCSP responder and optional URI to CA issuer certificate
Subject Alternative Name		Alternative name of the subscriber: email address
Key Usage	digitalSignature, nonRepudiation	Critical extension
Extended Key Usage		Optional Siehe Kapitel 6.1.7 für mögliche Werte
NsComment		Optional

Erweiterungsattribut	Werte	Anmerkung
Microsoft Certificate Template	(OID 1.3.6.1.4.1.311.20.2)	Optional

7.1.1.6 Erweiterungen des Swiss Post Platinum Verschlüsselungszertifikats für Organisationen

Erweiterungsattribut	Werte	Anmerkung
Subject	Daten des Antragsstellers	Siehe Definition in Kapitel 1.6
Issuer Name	/CN=Swiss Post Platinum CA – G2 /O=SwissSign AG/C=CH	
Authority Key Identifier	keyid: <key identifier of the issuing CA's public key>	Siehe Kapitel 7.1.3
CRL Distribution Points		URIs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy: 2.16.756.1.89.1.1.1.4.3 CPS: http://repository.swissign.com/Swiss-Post-Platinum-CP-CPS-R3.pdf	QCP public
Authority Information Access		URI to OCSP responder and optional URI to CA issuer certificate
Subject Alternative Name		Alternative name of the subscriber: email address
Key Usage	dataEncipherment, keyEncipherment	Critical extension
Extended Key Usage		Optional Siehe Kapitel 6.1.7 für mögliche Werte
NsComment		Optional
Microsoft Certificate Template	(OID 1.3.6.1.4.1.311.20.2)	Optional

8 Audit zur Einhaltung gesetzlicher Vorgaben und andere Beurteilungen

Die Bestimmungen und Bedingungen dieser CP/CPS sowie alle zugehörigen Regeln und Vorschriften werden zur Durchführung von Audits zur Einhaltung gesetzlicher Vorgaben bei folgenden Stellen verwendet:

- der Swiss Post Platinum CA;
- der Post RA.

8.1 Häufigkeit oder Voraussetzungen der Beurteilung

Das Audit zur Einhaltung gesetzlicher Vorgaben wird jährlich durchgeführt.

Es kann mehr als ein Audit zur Einhaltung gesetzlicher Vorgaben pro Jahr durchgeführt werden, wenn die auditierte Partei dies fordert oder ein vorangehendes Audit nicht zufrieden stellende Resultate ergeben hatte.

Die Audits für RA Post und SwissSign AG können unabhängig voneinander durchgeführt werden.

8.2 Identität/Qualifikationen des Auditor

Der CSO der SwissSign AG entscheidet, ob der Audit der SwissSign AG durch einen externen Auditor durchgeführt wird oder durch einen Mitarbeiter der SwissSign AG.

RA Post entscheidet selbständig, wer oder welche Organisation mit der Durchführung des Audit beauftragt wird.

Um als Auditor qualifiziert zu sein, müssen folgende Voraussetzungen gelten:

- Technisches PKI know-how
- Vertraut sein mit den entsprechenden Vorschriften (EIDI-V, TAV EIDI-V, TAV Bakom, ISO 27001, ETSI 101 456, etc.)

8.3 Beziehung des Auditor zur geprüften Stelle

Der Auditor der SwissSign AG ist vertraglich an die SwissSign AG gebunden. Entweder als Mitarbeiter oder durch einen Vertrag.

Der Auditor der RA Post ist vertraglich an die RA Post gebunden. Entweder als Mitarbeiter oder durch einen Vertrag.

8.4 Von der Beurteilung abgedeckte Themen

Der Auditor wählt die von der Beurteilung abzudeckenden Prüfziele gemäss den gesetzlichen Vorschriften aus.

8.5 Bei einem Mangel getroffene Massnahmen

Die SwissSign AG implementiert das ITIL Best Practices-Modell und die Resultate eines Audits zur Einhaltung gesetzlicher Vorgaben werden innerhalb dieses Rahmenwerks gehandhabt. Je nach Schwere und Dringlichkeit werden alle Sachverhalte in das ITIL-System eingegeben, entweder als Zwischenfälle oder als Probleme, und entsprechend verfolgt.

Durch Verwendung eines unterstützenden Hilfsmittels stellt die SwissSign AG sicher, dass alle Sachverhalte verfolgt und rechtzeitig behoben werden. Zu dem System gehören auch Berichte und eine Eskalation an das Management.

RA Post wählt situativ und in Absprache mit der SwissSign AG die geeignetsten Mittel um die Resultate des Audit zu dokumentieren und die geplanten Massnahmen umzusetzen.

8.6 Mitteilung der Resultate

Die Resultate des Audits von SwissSign AG zur Einhaltung gesetzlicher Vorgaben werden der Geschäftsführung der SwissSign AG innerhalb eines Monats mitgeteilt.

RA Post ist verpflichtet innerhalb eines Monats die Resultate des Audits und innerhalb von zwei Monaten einen Vorschlag für die Behebung der festgestellten Mängel an die SwissSign AG mitzuteilen.

SwissSign AG erstellt innert 30 Tagen nach dem Erhalt der Resultate der Audits zur Einhaltung gesetzlicher Vorgaben einen Vorschlag zuhanden der Post für die Behebung von festgestellten Mängeln der Audit Berichte von SwissSign AG und RA Post.

9 Sonstige geschäftliche und rechtliche Bestimmungen

9.1 Gebühren

Da die von dieser CA ausgegebenen Zertifikate ausschliesslich von der Post verkauft werden (vgl. Ziffer 1), kommen deren Preise zur Anwendung. Die Post stellt eine aktuelle Preisliste für Zertifizierungs- und Registrierungsdienste auf ihrer Website www.postzertifikat.ch zur Verfügung.

9.2 Finanzielle Verantwortung

Die diesbezüglichen Bestimmungen der CP/CPS „SwissSign Platinum CA“ finden Anwendung.

9.3 Vertraulichkeit von Geschäftsinformationen

Die diesbezüglichen Bestimmungen der CP/CPS „SwissSign Platinum CA“ finden Anwendung. Eine konzerninterne Weitergabe von Informationen ist im Rahmen der Leistungserbringung zulässig.

9.4 Vertraulichkeit von Personendaten

Die diesbezüglichen Bestimmungen der CP/CPS „SwissSign Platinum CA“ finden Anwendung. Eine konzerninterne Weitergabe von Informationen ist im Rahmen der Leistungserbringung zulässig.

9.5 Rechte des geistigen Eigentums

Die diesbezüglichen Bestimmungen der CP/CPS „SwissSign Platinum CA“ finden Anwendung.

9.6 Zusicherungen und Gewährleistungen

9.6.1 Zusicherungen und Gewährleistungen der Zertifizierungsstelle (CA)

SwissSign AG verpflichtet sich zur Einhaltung der Bestimmungen dieser CP/CPS und der Bestimmungen der CP/CPS „SwissSign Platinum CA“.

9.6.2 Zusicherungen und Gewährleistungen der Registrierungsstelle (RA)

Jede Registrierungsstelle verpflichtet sich zur Einhaltung der Bestimmungen dieser CP/CPS.

9.6.3 Zusicherungen und Gewährleistungen des Zertifikatsinhabers

Der Zertifikatsinhaber verpflichtet sich, alle Bestimmungen dieser CP/CPS sowie die Bestimmungen der anwendbaren AGB einzuhalten.

9.6.4 Zusicherungen und Gewährleistungen des Zertifikatsprüfers

Der Zertifikatsprüfer verpflichtet sich, alle Bestimmungen dieser CP/CPS einzuhalten.

9.6.5 Zusicherungen und Gewährleistungen anderer Teilnehmer

Andere Teilnehmer verpflichten sich, alle Bestimmungen dieser CP/CPS einzuhalten.

9.7 Gewährleistungsausschluss

Die diesbezüglichen Bestimmungen der CP/CPS „SwissSign Platinum CA“ finden Anwendung.

9.8 Haftung

9.8.1 Haftung der SwissSign AG

SwissSign AG haftet einzig für Schäden, die aufgrund ihres absichtlichen oder grobfahrlässigen Verhaltens entstehen.

Soweit gesetzlich zulässig, übernimmt die SwissSign AG keinerlei Haftung für entgangenen Gewinn, Datenverlust, mittelbare Schäden oder Folgeschäden. SwissSign AG haftet nicht für Schäden, welche dadurch verursacht werden, dass Zertifikatsinhaber oder Zertifikatsprüfer die anwendbaren Bestimmungen nicht einhalten.

Die SwissSign AG übernimmt keinerlei Haftung für Schäden, die durch höhere Gewalt (insbesondere Naturkatastrophen, Ausfall der Strom- oder Telekommunikationsnetze, unabwendbare Einwirkungen Dritter wie z.B. Viren- oder Hackerangriffe, staatliche Massnahmen) entstehen. Die SwissSign AG wird wirtschaftlich angemessene Massnahmen ergreifen, um die Auswirkungen höherer Gewalt rechtzeitig auf das Minimum zu beschränken. Schäden, die aufgrund einer Verzögerung entstehen, die durch Ereignisse höherer Gewalt verursacht wurden, werden nicht durch die SwissSign AG abgedeckt.

9.8.2 Haftung des Zertifikatsinhabers

Der Zertifikatsinhaber haftet für sämtlichen Schaden, der aus der Verletzung seiner aus Gesetz, Vertrag oder der vorliegenden CP/CPS resultierenden Verpflichtungen entsteht.

9.9 Schadenersatz

Die diesbezüglichen Bestimmungen finden sich unter Ziffer 9.8 des CP/CPS.

9.10 Inkrafttreten und Beendigung

9.10.1 Inkrafttreten

Diese CP/CPS sowie die jeweiligen Änderungen treten zum Zeitpunkt ihrer Veröffentlichung auf der Website der SwissSign AG unter „<http://repository.swissign.com>“ in Kraft.

9.10.2 Beendigung

Diese CP/CPS tritt mit der Veröffentlichung einer neuen Fassung auf der Website der SwissSign AG ausser Kraft.

9.10.3 Wirkung der Beendigung

Sämtliche Bestimmungen betreffend die Vertraulichkeit persönlicher und sonstiger Daten bleiben auch nach Beendigung weiterhin gültig.

9.11 Einzelbenachrichtigungen und Mitteilungen an Teilnehmer

Sofern nichts Gegenteiliges in dieser CP/CPS bestimmt ist, kann die SwissSign AG Benachrichtigungen über E-Mail, auf dem postalischen Weg, über Fax oder auf Webseiten bereitstellen.

9.12 Änderungen

Die SwissSign AG nimmt Änderungen an dieser CP/CPS nach Rücksprache mit der Post vor.

Neufassungen der CP/CPS treten mit ihrer Veröffentlichung auf der Website der SwissSign AG in Kraft und ersetzen alle früheren Fassungen dieser CP/CPS (vgl. Ziffer 9.10).

Bei Änderungen dieser CP/CPS mit Auswirkungen auf die Zertifikatsinhaber und/oder die Zertifikatsprüfer wird die OID dieser CP/CPS aktualisiert.

9.13 Beilegung von Streitigkeiten

Im Fall einer Streitigkeit oder Auseinandersetzung in Verbindung mit der Erfüllung, Durchführung oder Auslegung dieser CP/CPS werden sich die Parteien bemühen, zu einer gütlichen Einigung zu kommen.

9.14 Anwendbares Recht und Gerichtsstand

Anwendbar ist ausschliesslich schweizerisches Recht. Die Bestimmungen des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf vom 11. April 1980 (Wiener Kaufrecht) werden wegbedungen. Ausschliesslicher Gerichtsstand ist das Handelsgericht Zürich, Schweiz.

9.15 Einhaltung geltenden Rechts

Diese CP/CPS und alle damit verbundenen Rechte oder Pflichten sind in Übereinstimmung mit Schweizerischem Recht.

9.16 Sonstige Bestimmungen

9.16.1 Abtretung

Der Zertifikatsinhaber ist nicht berechtigt, seine Rechte oder Pflichten ganz oder teilweise abzutreten.

Die SwissSign AG ist berechtigt, ihre Rechte oder Pflichten ganz oder teilweise auf Dritte, insbesondere andere Konzerngesellschaften, zu übertragen.

9.16.2 Salvatorische Klausel

Werden einzelne Bestimmungen der CP/CPS von einem zuständigen Gericht als ungültig oder als nicht rechtskräftig angesehen, so wird die Gültigkeit der CP/CPS im Übrigen davon nicht berührt.

9.16.3 Sprache

Für rechtlich verbindliche Dokumente wie die CP/CPS, die Allgemeinen Geschäftsbedingungen oder die Registrierungsformulare ist die deutsche Fassung dieser Dokumente massgebend.