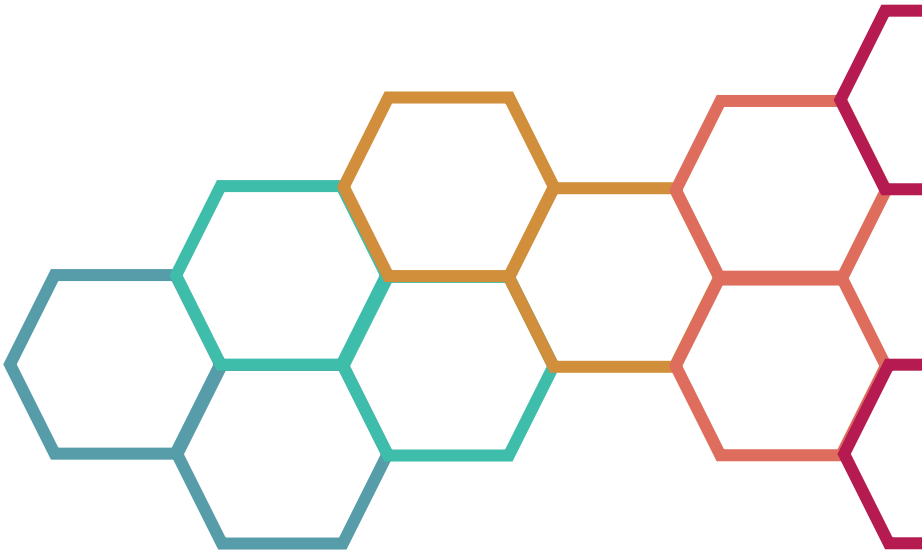
SIGN8 AG c/o SWISS COMPANY AG
Bahnhofstrasse 21
CH-6300 Zug

T: +41 (0)41 533 03 95
info@sign8.ch
www.sign8.ch

Certificate Practice Statement der SIGN8 AG



Version: 1.0
Datum: 15.01.2026

Unterschrift: Richard Ranftl

Digitally signed by Richard Ranftl
Date: 2026.01.27 00:59:43 +01'00'

(Geschäftsführer SIGN8 AG)

Dokumentationshistorie

Version	Anmerkung	Datum
1.0	Erstellung des Dokuments im Rahmen der Vorgaben nach ZertES und der ETSI-Standards.	15.01.2026

Referenzierte Dokumente

Kürzel	Beschreibung
[CPS eIDAS]	Certificate Practice Statement der SIGN8 GmbH
[Cert Profile ZertES]	Addendum zum CPS: Profile der Zertifikate und Online Statusabfragen (OCSP)

Inhalt

1. Einleitung 8
1.1. Überblick 8
1.1.1. Über dieses Dokument 9
1.1.2. Eigenschaften der PKI von SIGN8 9
1.2. Name und Kennzeichnung des Dokuments 10
1.3. PKI-Teilnehmer 10
1.3.1. Zertifizierungsstelle (CA) 10
1.3.2. Registrierungsstellen (RA) 10
1.3.3. Zertifikatsinhaber und Endanwender 11
1.3.4. Zertifikatsprüfer (Relying Party) 11
1.3.5. Andere Teilnehmer 11
1.3.6. Lizenznehmer 11
1.3.7. Unterzeichner 11
1.4. Verwendung von Zertifikaten 11
1.4.1. Gültigkeitsmodell 12
1.4.2. Verwendung von Dienstzertifikaten 12
1.5. Verwaltung der Konzepte 13
1.6. Definitionen und Abkürzungen 13
1.7. Übertragung von Aufgaben an Dritte 16
1.8. Ansprechpartner 16
2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen 17
2.1. Verzeichnisse 17
2.2. Veröffentlichung von Informationen zu Zertifikaten 17
2.3. Zeitpunkt und Häufigkeit von Veröffentlichungen 17
2.4. Zugang zu den Informationen 17
3. Identifizierung und Authentifizierung 18
3.1. Namensregeln 18
3.1.1. Arten von Namen 18
3.1.2. Aussagekraft von Namen 18
3.1.3. Pseudonyme 18
Pseudonyme werden angeboten. 18

3.1.4. Regeln für die Interpretation verschiedener Namensformen 18
3.1.5. Eindeutigkeit von Namen 18
3.1.6. Anerkennung, Authentifizierung und die Rolle von Markennamen 18
3.1.7. Password-Policy 18
3.1.8. Test-Zertifikate 19
3.2. Identifizierung der Zertifikatsinhaber 19
3.2.1. Nachweis über den Besitz des privaten Schlüssels 19
3.2.2. Identifizierung und Authentifizierung von UID-Einheiten 19
3.2.3. Identifizierung und Authentifizierung natürlicher Personen 20
3.2.4. Ungeprüfte Angaben zum Zertifikatsnehmer 21
3.2.5. Überprüfung fremder CAs, RAs 21
3.2.6. Prüfung der Berechtigung zur Antragsstellung 21
3.2.7. Interoperabilität 21
3.3. Identifizierung und Authentifizierung bei Anträgen auf Schlüsselerneuerung (re-keying) 21
3.4. Identifizierung und Authentifizierung bei Stellung eines Widerrufsverlangens 22
4. Betriebsanforderungen 23
4.1. Zertifikatsantrag 23
4.2. Verarbeitung des Zertifikatsantrags 23
4.2.1. Durchführung der Identifizierung und Authentifizierung 23
4.2.2. Annahme oder Ablehnung des Antrags 23
4.3. Ausstellung von Zertifikaten 23
4.3.1. Vorgehen der CA bei der Ausstellung des Zertifikats 23
4.3.2. Benachrichtigung des Zertifikatsinhabers über die Erstellung des Zertifikats 24
4.4. Zertifikatsübergabe 24
4.4.1. Verhalten bei der Zertifikatsübergabe 24
4.4.2. Veröffentlichung des Zertifikats durch den ZDA 24
4.4.3. Benachrichtigung Dritter über die Erstellung des Zertifikats 24
4.5. Verwendung des Schlüsselpaars und des Zertifikats 24
4.5.1. Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber 24
4.5.2. Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsinhaber 24
4.6. Zertifikatserneuerung 24
4.7. Zertifikatserneuerung mit Schlüsselerneuerung 24

4.8. Zertifikatsänderung 24
4.9. Widerruf und Suspendierung von Zertifikaten 24
4.9.1. Bedingungen für einen Widerruf 24
4.9.2. Widerrufsberechtigte 26
4.9.3. Verfahren zur Stellung eines Widerrufsverlangens 26
4.9.4. Fristen für ein Widerrufsverlangen 26
4.9.5. Zeitspanne für die Bearbeitung des Widerrufsverlangen 26
4.9.6. Methoden zum Prüfen von Widerrufsinformationen 26
4.9.7. Häufigkeit der Veröffentlichung von Widerrufslisten 27
4.9.8. Maximale Latenzzeit für Widerrufslisten 27
4.9.9. Online-Verfügbarkeit von Widerrufsinformationen 27
4.9.10. Notwendigkeit zur Online-Prüfung von Widerrufsinformationen 27
4.9.11. Andere Formen zur Anzeige von Widerrufsinformationen 27
4.9.12. Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels 27
4.9.13. Suspendierung des Zertifikats 27
4.10. Statusabfragedienst 27
4.11. Beendigung des Zertifizierungsdienstes 28
4.12. Schlüsselhinterlegung und -wiederherstellung 28
5. Nicht-technische Sicherheitsmassnahmen 29
5.1. Bauliche Sicherheitsmassnahmen 29
5.2. Verfahrensvorschriften 29
5.2.1. Rollenkonzept 29
5.2.2. Mehr-Augen-Prinzip 29
5.2.3. Sonstige Dienstanweisung 29
5.2.4. Standards und Kontrollen für kryptographische Module 29
5.3. Personalkonzept 29
5.3.1. Qualifikation, Erfahrung und Zuverlässigkeit des Personals 29
5.3.2. Sicherheitsüberprüfung 29
5.3.3. Schulungen und Weiterbildungen 29
5.3.4. Häufigkeit von Job-Rotation 29
5.3.5. Anforderungen an externes Personal 29
5.3.6. Sanktionen bei unerlaubten Handlungen 29
5.3.7. Dokumentation 30
5.4. Protokollierung von Überwachungsmassnahmen 30

5.4.1. Überwachung des Zutritts 30
5.4.2. Überwachung von organisatorischen Massnahmen 30
5.4.3. Art der aufgezeichneten Ereignisse 30
5.5. Archivierung von Unterlagen 30
5.5.1. Arten von Unterlagen 30
5.5.2. Aufbewahrungszeiten 30
5.5.3. Archivsicherheit 30
5.5.4. Datensicherung des Archivs 30
5.6. Umstellung des Schlüssels (key changeover) 30
5.7. Notfallkonzept 31
5.7.1. Behandlung von Vorfällen 31
5.7.2. Wiederherstellung von IT-Systemen 31
5.7.3. Wiederherstellung nach Kompromittierung von privaten CA-Schlüsseln 31
5.7.4. Weiterführung des Betriebs nach Kompromittierung oder Katastrophenfall 31
5.7.5. Regelmässige Kontrolle 31
5.8. Beendigung des Zertifizierungsbetriebs 31
6. Technische Sicherheitsmassnahmen 32
6.1. Erzeugung und Installation von Schlüsselpaaren 32
6.1.1. Erzeugung von Schlüsselpaaren 32
6.1.2. Auslieferung der privaten Schlüssel für Zertifikatsteilnehmer 32
6.1.3. Auslieferung der öffentlichen Schlüssel an die CA 32
6.1.4. Auslieferung der öffentlichen CA-Schlüssel 32
6.1.5. Schlüssellängen 32
6.1.6. Schlüsselparameter und Qualitätskontrolle der Parameter 32
6.1.7. Schlüsselverwendung 32
6.2. Schutz privater Schlüssel und technische Kontrollen kryptographischer Module 33
6.2.1. Standards und Sicherheitsmassnahmen 33
6.2.2. Schlüsselaktivierung 33
6.2.3. Schlüsselwiederherstellung 33
6.2.4. Schlüsselbackup 33
6.2.5. Schlüsselarchivierung 33
6.2.6. Schlüsseltransfer 33
6.2.7. Schlüsselspeicherung 33
6.2.8. Aktivierung privater Schlüssel 33

6.2.9. Deaktivierung privater Schlüssel 33
6.2.10. Zerstörung privater Schlüssel 34
6.2.11. Beschreibung der kryptografischen Module 34
6.3. Weitere Aspekte der Verwaltung des Schlüsselpaars 34
6.3.1. Archivierung der öffentlichen Schlüssel 34
6.3.2. Gültigkeitsdauer von Schlüssel und Zertifikaten 34
6.4. Aktivierungsdaten 34
6.4.1. Erzeugung und Installation von Aktivierungsdaten 34
6.4.2. Schutz von Aktivierungsdaten 34
6.4.3. Weitere Aspekte der Aktivierungsdaten 34
6.5. Computer-Sicherheitsmassnahmen 34
6.5.1. Spezifische technische Sicherheitsanforderungen an Computer-Systeme 34
6.5.2. Bewertung der Computersicherheit 34
6.6. Technische Kontrolle während des Lebenszyklus 34
6.6.1. Sicherheitsmassnahmen beim Aufbau, der Entwicklung und Erweiterung der IT-Systeme und Softwarekomponenten 34
6.6.2. Sicherheitsmassnahmen beim Computermanagement 35
6.6.3. Sicherheitsmassnahmen beim Betrieb 35
6.7. Netzwerksicherheit 35
6.8. Zeitstempel 35
6.9. API-Sicherheit 35
7. Profile von Zertifikaten, Widerrufslisten und OCSP 36
7.1 OIDs der genutzten Algorithmen 36
7.2 Certificate Revocation List Profile (CRL) 36
7.3 Status Query Service Profile (OCSP) 37
8. Konformitätsprüfung 38
8.1. Intervall oder Gründe von Prüfungen 38
8.2. Identität/Qualifikation des Prüfers 39
8.3. Beziehung des Prüfers zur prüfenden Stelle 39
8.4. Abgedeckte Bereiche der Prüfung 39
8.5. Massnahmen zur Mängelbeseitigung 39
8.6. Veröffentlichung von Ergebnissen 40
8.7. Nutzung des Vertrauenssiegel 40
9. Sonstige geschäftliche und rechtliche Regelungen 41
9.1. Preise 41

9.1.1. Preise für die Ausgabe von Zertifikaten 41
9.1.2. Gebühren für den Zugriff auf Zertifikate 41
9.1.3. Gebühren für den Widerruf von Zertifikaten oder den Erhalt von Statusinformationen 41
9.1.4. Gebühren für andere Dienstleistungen 41
9.1.5. Kostenrückerstattungen 41
9.2. Finanzielle Verantwortung 41
9.3. Vertraulichkeit von Geschäftsdaten 41
9.3.1. Definition von vertraulichen Geschäftsdaten 41
9.3.2. Geschäftsdaten die nicht vertraulich behandelt werden 41
9.3.3. Zuständigkeiten für den Schutz vertraulicher Geschäftsdaten 42
9.4. Schutz von Personendaten 42
9.4.1. Datenschutzkonzept 42
9.4.2. Definition von Personendaten 42
9.4.3. Nicht vertrauliche Daten 42
9.4.4. Verantwortung für den Schutz Personendaten 42
9.4.5. Hinweis und Einwilligung zur Nutzung von Personendaten 43
9.4.6. Erteilung von Auskünften im Rahmen von Gerichts- oder Verwaltungsverfahren 43
9.4.7. Andere Bedingungen für Auskünfte 43
9.5 Urheberrechte 43
9.5.1 ZDA 43
9.5.2. Zertifikatsnehmer 43
9.6. Zusicherungen, Garantien und Gewährleistung 43
9.7. Haftungsausschluss 44
9.8. Haftungsbeschränkung 44
9.9. Schadensersatz 44
9.10. Laufzeit und Beendigung 44
9.10.1. Gültigkeitsdauer des CPS 44
9.10.2. Beendigung der Dienste 44
9.10.3. Auswirkung der Beendigung 44
9.11. Mitteilungen an und Kommunikation mit Teilnehmern 45
9.12. Änderung des Zertifizierungskonzeptes 45
9.12.1. Verfahren für Änderungen 45
9.12.2. Benachrichtigungsverfahren und -fristen 45
9.12.3. Bedingungen für OID-Änderungen 45

9.13. Streitschlichtungsverfahren 45
9.14. Anwendbares Recht 45
9.15. Einhaltung geltenden Rechts 45
9.16. Sonstige Bestimmungen 45
9.16.1. Barrierefreiheit 45
9.16.2. Nichtdiskriminierungsklausel 46
9.16.3. Vollständigkeitserklärung 46
9.16.4. Abgrenzung 46
9.16.5. Salvatorische Klausel 46
9.16.6. Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht) 46
9.16.7. Höhere Gewalt 46
9.17. Andere Bestimmungen 46

1. Einleitung

1.1. Überblick

Dieses Dokument ist das Certification Practice Statement der SIGN8 AG, im Folgenden „SIGN8“ genannt.

Der Zertifizierungsdiensteanbieter, im Folgenden ZDA genannt, ist – auch im juristischen Sinne – die

SIGN8 AG
c/o SWISS COMPANY AG
Bahnhofstrasse 21
6300 Zug.

Der ZDA ist qualifizierter Zertifizierungsdiensteanbieter i.S.d. Abs. 2 Art. 3 des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, [ZertES]), sowie SSASP nach ETSI TS 119 431-1.

Teilaufgaben des ZDA werden an Partner oder externe Anbieter ausgelagert.

Für die Einhaltung der Verfahren im Sinne dieses Dokuments bzw. etwaiger gesetzlicher oder zertifizierungstechnischer Anforderungen an den ZDA, bleibt der ZDA, vertreten durch die Geschäftsführung oder deren Beauftragte, verantwortlich.

Der ZDA bietet die Ausstellung von qualifizierten und geregelten Zertifikaten für qualifizierte elektronische Signaturen und geregelte Siegel im Sinne des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (ZertES) und der zugehörigen Verordnung über die elektronische Signatur, [VZertES]) an. Qualifizierte und geregelte Zertifikate werden ausschliesslich über die beim ZDA betriebenen CAs ausgestellt und benötigen zur Erstellung eine QSCD gemäss den regulatorischen Vorgaben.

Die für den Fernsignatur- und Fernsiegeldienst ausgestellten qualifizierten und geregelten Zertifikate, auch Fern-Zertifikate genannt, können zur Erstellung von qualifizierten elektronischen Fernsignaturen und geregelten Fernsiegel verwendet werden.

Die geregelten Fernsiegel können ausschliesslich von UID-Einheiten angewendet werden. Die qualifizierte Fernsignaturen können ausschliesslich von natürlichen Personen angewendet werden.

Der ZDA stellt auch Zertifikate für eigene Zwecke aus. Hierbei werden ebenfalls die entsprechenden gesetzlichen bzw. zertifizierungstechnischen Anforderungen eingehalten.

1.1.1. Über dieses Dokument

Dieses CPS definiert Abläufe und Vorgehensweisen, während der gesamten Lebensdauer der qualifizierten und geregelten Zertifikate bis zu deren Archivierung, für den Zertifizierungsdienst der Ausstellung von qualifizierten und geregelten Zertifikaten für qualifizierte elektronische Signaturen und geregelte Siegel im Sinne des ZertES (943.03), VZertES (943.032), TAV (943.032.1), ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-1 bis ETSI EN 319 412-5 sowie DIN EN 419 241. Es werden Mindestmassnahmen festgelegt, die von allen PKI-Teilnehmern zu erfüllen sind. Des Weiteren beinhaltet dieses Zertifizierungskonzept das SCP, definiert in ETSI TS 119 431-1.

Die Gliederung des Zertifizierungskonzepts basiert auf dem Standard RFC 3647, um einen Vergleich mit den Zertifizierungskonzepten anderer Zertifizierungsdiensteanbieter zu erleichtern.

Massgeblich ist allein die deutsche Fassung dieses Zertifizierungskonzepts.

Als alleinstehendes Dokument ist dieses Zertifizierungskonzept im Verhältnis zwischen dem ZDA und dem Zertifikatsinhaber bzw. der Relying Party rechtsverbindlich. Für das Verhältnis zwischen dem ZDA und dem Zertifikatsinhaber bzw. der Relying Party sind ebenso die vertraglichen, oder bei Fehlen eines Vertragsverhältnisses, die gesetzlichen Bestimmungen, sowie die wirksam einbezogenen AGB massgeblich. Soweit nicht ausdrücklich anders vermerkt, beinhaltet dieses Zertifizierungskonzept keine Zusicherungen, Garantien oder Gewährleistungen. In Bezug auf das Verhältnis zwischen der Konformitätsbewertungsstelle und dem ZDA ist dieses Dokument ebenso rechtsverbindlich.

1.1.2. Eigenschaften der PKI von SIGN8

Die PKI des ZDA ist mehrstufig aufgebaut und besteht aus einer Root-CA, welche auf einem selbst-signierten Wurzel-Zertifikat basiert und daraus abgeleiteten Subordinate-CAs. Endanwender-Zertifikate werden jeweils von den Subordinate-CAs signiert.

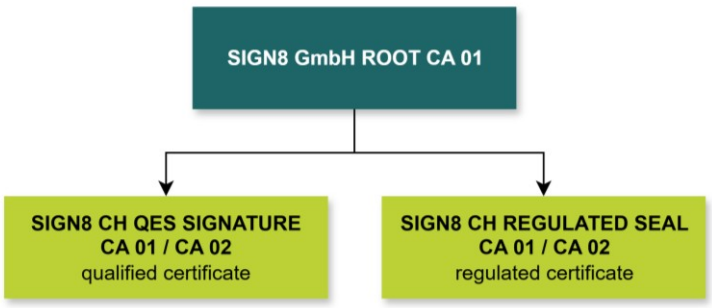


Abbildung 1: PKI-Hierarchie der PKI des ZDA

Die ausgegebenen Zertifikate entsprechen den Anforderungen des ZertES. Alle ausgegebenen Zertifikate lassen sich bis zum Wurzel-Zertifikat prüfen und wurden in einer zertifizierten QSCD innerhalb eines sicheren Rechenzentrums (Trust Center) erstellt. Zur Generierung der Schlüssel kommen ausschliesslich zertifizierte QSCDs zum Einsatz. Die Gültigkeit der Zertifizierung der eingesetzten QSCDs wird regelmässig geprüft. Vor Ablauf einer Zertifizierung wird rechtzeitig der Einsatz einer anderen zertifizierten QSCD geplant und umgesetzt.

Die Zertifikate entsprechen zusätzlich den Anforderungen der ETSI Standards EN 319 401, EN 319 411-1, EN 319 411-2, EN 319 412-1, EN 319 412-2, EN 319 412-3, EN 319 412-4, EN 319 412-5, DIN EN 419 241-1 und TS 119 431-1.

Die hier aufgeführte PKI wird ausschliesslich von der SIGN8 GmbH betrieben.

1.2. Name und Kennzeichnung des Dokuments

Dokumentenname: Certificate Practice Statement der SIGN8 AG

Kennzeichnung: 1.3.6.1.4.1.63345.2.4.0

Version: 1.0

Bei Änderungen an diesem Dokument (CPS/SCP), die den Geltungsbereich des Dokuments beeinflussen, wird die Version entsprechend angepasst.

Die angebotenen Dienste entsprechen den folgenden Service-Identifiern:

- URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC
- URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC
- URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSCDManagement/Q

1.3. PKI-Teilnehmer

1.3.1. Zertifizierungsstelle (CA)

Die Zertifizierungsstelle (auch die ***Certificate Authority*** – kurz die ***CA***) stellt Zertifikate aus und erteilt Auskünfte zu deren Status.

1.3.2. Registrierungsstellen (RA)

Die Registrierungsstelle (auch die ***Registration Authority*** – kurz die ***RA***) identifiziert und authentifiziert die Zertifikatsinhaber, erfasst und prüft Anträge der Zertifikatsinhaber auf Erbringung von Vertrauensdienstleistungen durch die Zertifizierungsstelle. Anträge auf Widerruf der von der CA ausgegebenen Zertifikate werden ebenfalls von der Registrierungsstelle erfasst, geprüft und an die CA weitergeleitet.

1.3.3. Zertifikatsinhaber und Endanwender

Zertifikatsinhaber (auch der ***Subscriber***) sind natürliche Personen, die von der Zertifizierungsstelle ausgegebene Zertifikate innehaben. Endanwender (auch das ***Subject*** oder ***End Entity***) verwenden die ausgegebenen Zertifikate. Der Endanwender und der Zertifikatsinhaber sind dieselbe Person. Ausgenommen hiervon sind geregelte Siegelzertifikate, welche für UID-Einheiten ausgestellt werden.

1.3.4. Zertifikatsprüfer (Relying Party)

Relying Parties sind natürliche oder UID-Einheiten oder sonstige Dritte (z.B. Systeme), welche die Zertifikate der PKI der SIGN8 AG nutzen und Zugang zu den Zertifizierungsdienstleistungen der SIGN8 AG haben.

1.3.5. Andere Teilnehmer

Andere Teilnehmer sind Dritte, auf die der ZDA, Funktionen und/oder Aufgaben übertragen hat (die ***Anderen Teilnehmer***).

Der ZDA hat Aufgaben der Zertifizierungs- bzw. Registrierungsstelle auf Dritte übertragen. Eine genaue Auflistung aller externen Dienstleister kann in den TOM eingesehen werden.

1.3.6. Lizenznehmer

Personen, die Abonnent einer der angebotenen SIGN8-Produkte (auch die ***SIGN8 Lösungen***) sind und ein Kundenkonto bei SIGN8 besitzen. Die Abonnenten von SIGN8 haben die Möglichkeit über die Website von SIGN8 aus einem nutzerbasierten oder volumenbasiertem Abonnementmodell zu wählen. Je nach Abonnementmodell erhält der Lizenznehmer Zugriff auf die jeweiligen SIGN8 Lösungen.

Lizenznehmer sind ausserdem alle Personen, die mit dem ZDA einen Vertrag über den Betrieb einer SIGN8 TCI geschlossen haben.

Ferner sind Lizenznehmer Personen, die einen SIGN8 Token über die SIGN8 Website bestellen.

1.3.7. Unterzeichner

Unterzeichner sind natürliche Personen, welche durch Einwilligung der ihnen zur Verfügung gestellten AGB, SIGN8 den Auftrag geben qualifizierte und geregelte Zertifikate in ihrem Namen auszustellen. Unterzeichner haben die Möglichkeit mithilfe des angebotenen Zertifizierungsdienst, qualifizierte Fernsignaturen und geregelte Fernsiegel zu erstellen. Alle Unterzeichner sind Zertifikatsinhaber und Endanwender.

1.4. Verwendung von Zertifikaten

Zertifikatsinhaber dürfen, die von dem ZDA ausgegebenen qualifizierten und geregelten Zertifikate nur in zulässigen und geltenden gesetzlichen Rahmen nutzen. Sie handeln insoweit

auf eigene Verantwortung. Die Einschätzung, ob dieses Zertifizierungskonzept den Anforderungen einer Anwendung entspricht und ob die Benutzung des betreffenden qualifizierten oder geregelten Zertifikats zu einem bestimmten Zweck geeignet ist, obliegt dem Zertifikatsinhaber. Der ZDA übernimmt keine Haftung für den Fall, dass ein Zertifikatsinhaber ein qualifiziertes oder geregeltes Zertifikat zu anderen als dem zulässigen Zwecken nutzt.

Ferner unterliegt der Zertifikatsinhaber den sich aus den gesetzlichen Regelungen ergebenden Pflichten, zudem ggf. weitergehenden oder abweichenden Pflichten aufgrund einzelvertraglicher Regelung sowie den AGB der SIGN8 AG.

Es werden keine Attribute, welche über die Angaben im Abschnitt *3. Identifizierung und Authentifizierung* und *7. Profile von Zertifikaten, Widerrufslisten und OCSP* hinausgehen, angeboten.

1.4.1. Gültigkeitsmodell

Ab Inbetriebnahme der ZertES-konformen Zertifizierungshierarchie gilt für Endanwenderzertifikate das Schalenmodell. Das Schalenmodell besagt, dass alle Zertifikate zum Zeitpunkt der zu prüfenden Signatur gültig gewesen sein müssen. Das bedeutet, dass zum Signaturzeitpunkt eines Dokumentes alle Zertifikate in der Zertifikatshierarchie gültig gewesen sein müssen.

1.4.2. Verwendung von Dienstzertifikaten

Dienstzertifikate werden durch den ZDA selbst und zur eigenen Verwendung ausgestellt. Sie unterliegen den Anforderungen der jeweilig anwendbaren Zertifizierung. Zu den Verwendungsarten zählen:

- CA-Zertifikate zur CA- und Zertifikatserstellung;
- Signatur von Sperrauskünften (OCSP).

Die Dienstzertifikate (bzw. Infrastruktur- und Kontrollschlüssel) werden nur für ihren vorgesehenen Zweck benutzt.

1.5. Verwaltung der Konzepte

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

Den für die Verwaltung zuständigen Ansprechpartner können Sie unter folgender Adresse erreichen:

SIGN8 AG
c/o SWISS COMPANY AG
Bahnhofstrasse 21
6300 Zug.
Tel.: +41-41 533 03 95
E-Mail: info@sign8.ch

1.6. Definitionen und Abkürzungen

Begriff	**Beschreibung/Definition**
AGB	Allgemeine Geschäftsbedingungen für den Zertifizierungsdienst
Akkreditierungsstelle	Bereich des SECO (Staatssekretariat für Wirtschaft), der Aufsichtsaufgaben in der Schweiz wahrnimmt (u.a. Akkreditierung von Anerkennungsstellen).
Anerkennungsstelle	Stelle, die nach Bundesgesetzgebung für die Anerkennung und Überwachung der Anbieter von Zertifizierungsdiensten (ZDA) akkreditiert ist (in CH: SAS).
API	Application Programming Interface
Andere Teilnehmer	Siehe Abschnitt *1.3.5. Andere Teilnehmer*
BMA	Brandschutzmeldeanlage
BAKOM	Bundesamt für Kommunikation
CA/Certificate Authority	Zertifizierungsstelle
CPS	Certification Practice Statement
EMA	Einbruchmeldeanlage
Endanwender	Subject, die Identität des Endanwenders ist mit dem Zertifikat und dem zugehörigen Schlüsselpaar verknüpft, siehe auch Abschnitt *1.3.3. Zertifikatsinhaber und Endanwender*

EE	End-Entity sind alle Unterzeichner
EE-Zertifikate	End-Entity-Zertifikate sind Zertifikate, welche für die Endanwender der Sign8 PKI ausgestellt werden. EE-Zertifikate sind nicht in der Lage selbst Zertifikate auszustellen.
HSM	Hardware Security Module
Inhaltsdaten	Informationen über den Antragsteller, die in ein qualifiziertes oder geregeltes Zertifikat übernommen werden.
OCSP	Online Certificate Status Protocol
OTP	One-Time Password
Passkeys	Aufbauend auf FIDO2: kryptografische Schlüsselpaare, die zur Authentifizierung ohne Passwort dienen, indem sie die Benutzeridentität durch einen privaten Schlüssel auf dem Gerät und einen öffentlichen Schlüssel auf dem Server sichern und i.d.R. Biometrie zur Authentisierung verwenden.
PKI	Public Key Infrastructure
PDS	PKI Disclosure Statement
QCP-l-QSCD	Qualifizierte Zertifikatsrichtlinie für qualifizierte Zertifikate, die an juristische Personen ausgegeben werden, die über einen privaten Schlüssel für den zertifizierten öffentlichen Schlüssels in einer QSCD verfügen
QCP-n-QSCD	Qualifizierte Zertifikatsrichtlinie für qualifizierte Zertifikate, die an natürliche Personen ausgegeben werden, die über einen privaten Schlüssel für den zertifizierten öffentlichen Schlüssels in einer QSCD verfügen
QSCD	qualifizierte elektronische Signaturerstellungseinheit, die die Anforderungen nach der TAV erfüllen
RA/Registration Authority	Siehe Registrierungsstelle, Abschnitt *1.3.2. Registrierungsstellen (RA)*
Relying Party	Siehe Abschnitt *1.3.4. Zertifikatsprüfer (Relying Party)*
Root-CA	Oberste Zertifizierungsinstanz einer PKI
SAD	Signatur-Aktivierungsdaten
SCP	SSASC Policy
CPS	Service Provision Practice Statement
SSASC	Server Signing Application Service Component

SSASP	Server Signing Application Service Provider
Suspendierung	Vorrübergehendes Sperren eines Zertifikates mit der Möglichkeit das Zertifikat nach einer bestimmten Zeit wiederherzustellen.
TAV	Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (TAV)
TCI	Trust Center Infrastruktur, eine vom ZDA betriebene QSCD und weiteren Komponenten, die exklusiv für einen Lizenznehmer betrieben wird
Token	Eine lokale QSCD in Form eines USB-Sticks oder einer Smartcard
TOM	Technisch-Organisatorische Massnahmen
Trust Center	Rechenzentrum, in dem alle sicherheitsrelevante Hard- und Software untergebracht ist.
TP	Timestamping Policy
TW4S	Vertrauenswürdige Serversignaturen-System
UID-Einheit	UID-Einheit nach Artikel 3 Absatz 1 Buchstabe c des Bundesgesetzes vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer (UIDG). Hauptsächlich: - UID-Einheiten - Personengesamtheiten ohne Rechtsfähigkeit (z.B. einfache Gesellschaft) - Einzelfirmen - gewisse Verwaltungseinheiten von Bund, Kantonen, Bezirken und Gemeinden
UIDG	Bundesgesetz über die Unternehmens-Identifikationsnummer
UUID	Universally unique identifier
ZDA	Zertifizierungsdiensteanbieter: Anbieter von Zertifizierungsdiensten entsprechend Art. 2 Buchstabe k ZertES
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Verordnung über die elektronische Signatur, VZertES)

ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES)
Zertifizierungsdienst	Elektronischer Dienst entsprechend Art. 2 Buchstabe k ZertES
Zertifikat	qualifiziertes Zertifikat für elektronische Signaturen i. S. d. Art. 2 Buchstabe g und h ZertES
Zertifikatsinhaber	Siehe Abschnitt *1.3.3. Zertifikatsinhaber und Endanwender*
Zertifizierungsstelle	Siehe Abschnitt *1.3.1. Zertifizierungsstelle (CA)*

1.7. Übertragung von Aufgaben an Dritte

Die Gesamtverantwortung für die angebotenen Zertifizierungsdienste liegt beim ZDA SIGN8 AG. Die Übertragung von Aufgaben an Dritte erfolgt auf der Grundlage und nach Massgabe einer privatrechtlichen Vereinbarung. Die vertraglichen Vereinbarungen gewährleisten, dass die aus der Aufgabenübertragung resultierenden gesetzlichen Anforderungen und die Regelungen des Zertifizierungskonzepts und des Notfallkonzeptes eingehalten werden. Die Aufgaben und Pflichten der Dritten sind in der jeweiligen vertraglichen Vereinbarung festgelegt.

Die Dritten verpflichten sich, zur Erfüllung der ihnen von dem ZDA übertragenen Aufgaben ausschliesslich zuverlässige, ausreichend geschulte und fachkundige Mitarbeiter einzusetzen.

Der ZDA überträgt die Verantwortung der Übertragung von Aufgaben an Dritte der SIGN8 GmbH.

1.8. Ansprechpartner

Anfragen an den ZDA richten Sie bitte an:

SIGN8 AG
c/o SWISS COMPANY AG
Bahnhofstrasse 21
6300 Zug
Tel.: +41-41 533 03 95
E-Mail: info@sign8.ch

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1. Verzeichnisse

Der ZDA stellt einen Online-Dienst (***OCSP***) zur Abfrage der Validität der von dem ZDA ausgegebenen Zertifikate zur Verfügung.

Weiterhin können alle CA-Zertifikate und Beispiel-EE-Zertifikate des ZDA auf der Webseite des ZDA unter: https://sign8.ch/trust abgerufen werden.

2.2. Veröffentlichung von Informationen zu Zertifikaten

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben. Diese gelten sowohl für qualifizierte und geregelte Zertifikate.

2.3. Zeitpunkt und Häufigkeit von Veröffentlichungen

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

2.4. Zugang zu den Informationen

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

3. Identifizierung und Authentifizierung

3.1. Namensregeln

3.1.1. Arten von Namen

Qualifizierte und geregelte elektronische Zertifikate müssen den Namen oder ein Pseudonym des Endanwenders enthalten. Die Zertifikate entsprechen dem Profil des Standards ITU-T Recommendation X.509v3. Zertifikate für natürliche Personen enthalten den Namen zusammengesetzt aus Vor- und Familiennamen oder ein Pseudonym. Zertifikate für UID-Einheiten enthalten die offizielle Bezeichnung der UID-Einheit. Die Identität des Zertifikatsinhabers und der Endanwender wird überprüft.

3.1.2. Aussagekraft von Namen

Die verwendeten Zertifikate sind eindeutig innerhalb dieser PKI. Um dies sicherzustellen, enthält jedes Zertifikat das Feld serialNumber mit einer einmalig vergebenen UUID.

3.1.3. Pseudonyme

Pseudonyme werden angeboten.

3.1.4. Regeln für die Interpretation verschiedener Namensformen

Die Attribute von EE-Zertifikaten für natürliche Personen und UID-Einheiten werden im Abschnitt *7. Profile von Zertifikaten, Widerrufslisten und OCSP* aufgeführt.

3.1.5. Eindeutigkeit von Namen

Die Eindeutigkeit des Zertifikats wird mittels der Seriennummer (serialNumber) erzielt. Der ZDA stellt die Eindeutigkeit von serialNumber in CA-Zertifikaten sicher.

3.1.6. Anerkennung, Authentifizierung und die Rolle von Markennamen

Der Antragsteller verpflichtet sich zur Einhaltung geistiger Eigentumsrechte in den Antrags- und Zertifikatsdaten. Der Endanwender trägt die Verantwortung für die Vereinbarkeit der Namenswahl mit den Rechten Dritter, z.B. Namens-, Marken-, Urheber- oder sonstigen Schutzrechten, sowie mit den allgemeinen Gesetzen. Der ZDA ist nicht verpflichtet, solche Rechte zu überprüfen. Daraus resultierende Schadenersatzansprüche gehen zu Lasten des Endanwenders.

3.1.7. Password-Policy

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

3.1.8. Test-Zertifikate

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

3.2. Identifizierung der Zertifikatsinhaber

Der ZDA hat Personen, die ein qualifiziertes Zertifikat beantragen, eindeutig zu identifizieren. Dabei werden nur Informationen erfasst, die zur Nutzung des Dienstes und zur Erstellung der Zertifikate notwendig sind.

3.2.1. Nachweis über den Besitz des privaten Schlüssels

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

3.2.2. Identifizierung und Authentifizierung von UID-Einheiten

Um die UID-Einheit, die im Distinguished Name (DN) des Zertifikats unter *Organization (O)* genannt wird, zu identifizieren, wird die jeweilige UID-Nummer (Unternehmens-Identifikationsnummer) und/oder die Handelsregisternummer zur Nachprüfung benötigt.

Die Identität der UID-Einheit sowie die Berechtigung der handelnden Personen müssen gemäss Art. 6 Abs. 1 der VZertES i.V.m. Art. 9 ZertES verifiziert werden.

Für alle Rechtsformen werden folgende Daten erhoben:

1. Firma, Name oder Bezeichnung gemäss offiziellem Register,
2. Rechtsform,
3. Unternehmens-Identifikationsnummer (UID) und, falls vorhanden, Handelsregisternummer (CH-ID),
4. Anschrift des Sitzes oder der Hauptniederlassung (Domiziladresse),
5. Namen der gesetzlichen Vertreter (Organe) gemäss Registereintrag,
6. E-Mail-Adresse zur direkten Kontaktaufnahme durch den ZDA.

Für alle Rechtsformen wird in jedem Fall überprüft und eingefordert:

1. Existenz und Status der UID-Einheit (Register-Nachweis):
    - Ist die UID-Einheit im Handelsregister eingetragen, muss ein aktueller und beglaubigter Auszug aus dem Handelsregister (oder einem gleichwertigen amtlichen Register) vorgelegt werden.
    - Hat die UID-Einheit der Veröffentlichung ihrer Daten im UID-Register widersprochen (gemäss Art. 11 Abs. 3 UIDG), ist zwingend ein aktueller und beglaubigter Auszug aus dem UID-Register vorzulegen.
2. die Autorisierung des Vertreters des Antragsstellers der im Auftrag aufgeführten UID-Einheit:
    - Sofern bei nicht alleiniger Zeichnungsberechtigung: Schriftliche Vollmacht des geschäftsführenden Organs oder von zwei kollektiv zeichnungsberechtigten

Personen. Einzelunterschrift wird nur akzeptiert, wenn Einzelzeichnungsberechtigung im Handelsregisterauszug vermerkt ist.
- Bei nicht im Handelsregister eingetragenen Organisationen: Schriftliche Vollmacht zum Zertifikatsantrag, ausgestellt vom obersten Organ der Antragstellerin.

Für die Überprüfung der Existenz, der Adresse oder weiterer oben genannter Angaben der UID-Einheit werden ausschliesslich die Handelsregisterauszüge, vergleichbare Verzeichnisse oder amtliche Bestätigungen herangezogen. Online abgerufene Register und Verzeichnisse werden dabei ausschliesslich über HTTPS aufgerufen.

Mindestens ein juristischer Vertreter wird durch einen zertifizierten Identifizierungsdienstleiser im Auftrag des ZDA gemäss Abschnitt *3.2.3. Identifizierung und Authentifizierung natürlicher Personen* identifiziert.

Existiert ein gültiges Zertifikat, kann die Authentifizierung jeder siegelberechtigten Person einer UID-Einheit für die Transaktion durch eine, durch den ZDA zugelassene, Authentifizierungsmethode erfolgen.

Bei erstmaliger Identifizierung erstellen die siegelberechtigten Personen ein Konto bei SIGN8 und hinterlegen eine 2FA Methode. Das Siegel wird mit dem SIGN8 Konto verknüpft und ist somit über die Zugangsdaten und den hinterlegten 2FA Methoden geschützt.

Eine Authentifizierung bei einem SIGN8 Token erfolgt durch den Besitz des Tokens und der Eingabe einer PIN.

3.2.3. Identifizierung und Authentifizierung natürlicher Personen

Die Identität einer natürlichen Person muss gemäss Art. 9 ZertES i.V.m. Art. 5 Abs. 1 und Art. 7 VZertES verifiziert werden. Dies umfasst ebenso den Vertretungsberechtigten des Endanwenders. Es ist möglich Identitätsdaten zu nutzen, die zu einem früheren Zeitpunkt erhoben wurden.

Der ZDA nutzt für die Identifizierung des Unterzeichners Verfahren gemäss Kap. 2.3.1 Buchstabe a) der TAV, sofern nicht bereits ein gültiges Zertifikat existiert. Die Identifizierung des Unterzeichners erfolgt durch vom ZDA beauftragte externe Identifizierungsdienstleister gemäss Art. 9 Abs. 5 ZertES oder SIGN8 Ident Agenturen. Der Unterzeichner wird über einen gesicherten Kanal an den ausgewählten Identifizierungsdienstleister weitergeleitet.

Folgende Daten werden gemäss den Vorgaben der VZertES und der TAV von den beauftragten Dritten erhoben und protokolliert:

Mindestens:

- Vor- und/oder Nachname bzw. Pseudonym

- Geburtsdatum und Geburtsort (bzw. Heimatort bei Schweizer Ausweisdokumenten)
- Staatsangehörigkeit
- Ausweisdaten (Art, Nummer, ausstellende Behörde und Gültigkeit)

Optional:

- Wohnsitz / Meldeadresse
- E-Mail-Adresse
- Telefon- und Mobilfunknummer

Existiert ein gültiges Zertifikat, erfolgt die Authentifizierung des Unterzeichners für die Transaktion durch eine, durch den ZDA zugelassene, Authentifizierungsmethode.

Eine Authentifizierung bei einem SIGN8 Token erfolgt durch den Besitz des Tokens und der Eingabe einer PIN.

3.2.4. Ungeprüfte Angaben zum Zertifikatsnehmer

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

3.2.5. Überprüfung fremder CAs, RAs

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

3.2.6. Prüfung der Berechtigung zur Antragsstellung

Berechtigt zur Antragsstellung für Zertifikate ist jede geschäftsfähige natürliche Person.

Im Rahmen der Ausstellung von Siegelzertifikaten werden geregelte Zertifikate ausschliesslich für UID-Einheiten (Endanwender) ausgestellt. Der Endanwender muss dem ZDA gegenüber seinen Existenznachweis nach Abschnitt *3.2.2. Identifizierung und Authentifizierung von UID-Einheiten* erbringen, die Vertretungsberechtigung des Zertifikatsnehmers nachweisen, sowie den Identitätsnachweis ggf. mit UID-Einheitszugehörigkeit des Zertifikatnehmers nach den Abschnitten *3.2.2. Identifizierung und Authentifizierung von UID-Einheiten* und *3.2.3. Identifizierung und Authentifizierung natürlicher Personen* erbringen. Nach der Prüfung der Antragsdokumente entscheidet der ZDA, ob er den Antrag annimmt oder ablehnt.

3.2.7. Interoperabilität

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

3.3. Identifizierung und Authentifizierung bei Anträgen auf Schlüsselerneuerung (re-keying)

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

3.4. Identifizierung und Authentifizierung bei Stellung eines Widerrufsverlangens

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

4. Betriebsanforderungen

4.1. Zertifikatsantrag

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

4.2. Verarbeitung des Zertifikatsantrags

4.2.1. Durchführung der Identifizierung und Authentifizierung

Der beschriebene Identifizierungs- und Authentifizierungsprozess muss vollständig durchlaufen werden und alle nötigen Nachweise und Dokumente müssen erbracht werden.

Die Identifikation und Authentifikation der Antragssteller wird durch von dem ZDA beauftragten externen Identifizierungsdienstleister oder SIGN8 Ident Agenturen. Alle Identifikationsdienstleister werden in den TOM aufgeführt.

Ein erfolgreich abgeschlossener SIGN8 Ident Identifizierungsvorgang kann zur Bestätigung von bereits gestellten und zukünftigen Zertifikatsanträgen verwendet werden. In beiden Fällen werden die Identifikationsmerkmale Nachname, Vorname, Geburtsdatum und zusätzlich die E-Mail-Adresse überprüft. Weiterhin dürfen zwischen dem Tag der Antragsstellung und dem Tag der Identifizierung, nicht mehr als 30 Tage liegen. Der Antragsteller bestätigt ausserdem, die andauernde Korrektheit der im Identifizierungsvorgang erhobenen Daten und autorisiert den Vorgang mithilfe einer durch den ZDA zugelassenen Methode.

Der ZDA ist für die ordentliche Identifizierung nach Art. 9 Absatz 5 und 6 des ZertES verantwortlich. Dieser muss mindestens das Sicherheitsniveau „substanziell“ ausweisen gemäss EN 419 241-1.

Die Identifizierung und Authentifizierung der Antragsteller sowie die Prüfung weiterer zertifikatsrelevanter Daten muss vor der Ausstellung eines Zertifikats abgeschlossen und alle nötigen Nachweise und Dokumente müssen erbracht worden sein.

Durch dieses Vorgehen wird sichergestellt, dass die ausgestellten Zertifikate für elektronische Signaturen und Siegel gemäss Art. 7 Abs. 4 und Art. 8 Abs. 4 ZertES, sowie Art. 4 und 5 VZertES eindeutig dem Zertifikatsinhaber und Unterzeichner zugeordnet werden können und der Unterzeichner eindeutig identifiziert werden kann.

4.2.2. Annahme oder Ablehnung des Antrags

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

4.3. Ausstellung von Zertifikaten

4.3.1. Vorgehen der CA bei der Ausstellung des Zertifikats

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

4.3.2. Benachrichtigung des Zertifikatsinhabers über die Erstellung des Zertifikats

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

4.4. Zertifikatsübergabe

4.4.1. Verhalten bei der Zertifikatsübergabe

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

4.4.2. Veröffentlichung des Zertifikats durch den ZDA

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

4.4.3. Benachrichtigung Dritter über die Erstellung des Zertifikats

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

4.5. Verwendung des Schlüsselpaars und des Zertifikats

4.5.1. Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

4.5.2. Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsinhaber

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

4.6. Zertifikatserneuerung

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

4.7. Zertifikatserneuerung mit Schlüsselerneuerung

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

4.8. Zertifikatsänderung

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

4.9. Widerruf und Suspendierung von Zertifikaten

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

4.9.1. Bedingungen für einen Widerruf

Betroffene Dritte, Zertifikatsinhaber oder eine sonstige dritte Partei, sind aufgefordert, den Widerruf unverzüglich zu beantragen, wenn der Verdacht besteht, dass private Schlüssel kompromittiert wurden, die Kontrolle und der Zugriff (z.B. Authentifizierungsdaten) über den

privaten Schlüssel kompromittiert wurden oder Inhaltsdaten des Zertifikats nicht mehr korrekt sind.

In folgenden Fällen erfolgt ein Widerruf des Zertifikats durch den ZDA:

- auf Verlangen des Zertifikatsinhabers, oder der BAKOM;
- bei Ungültigkeit oder Unwahrheit von Angaben im Zertifikat;
- bei Beendigung der Tätigkeit als Zertifizierungsdiensteanbieter, wenn diese nicht von einem anderen qualifizierten und geregelten Zertifizierungsdiensteanbieter fortgeführt wird.

Der ZDA widerruft Zertifikate insbesondere auch dann, wenn

- das Vertragsverhältnis gekündigt wurde;
- wenn Tatsachen die Annahme rechtfertigen, dass (i) das Zertifikat gefälscht oder nicht hinreichend fälschungssicher ist oder (ii) die verwendeten qualifizierten und geregelten elektronischen Signaturerstellungseinheiten Sicherheitsmängel aufweisen;
- der private Schlüssel der ausstellenden oder der übergeordneten CA kompromittiert wurde;
- der Zertifikatsinhaber eine Zerstörung seines privaten Schlüssels verlangt;
- der Antrag des Zertifikatsinhabers aufgrund eines Rahmenvertrages erfolgt ist und dieser Rahmenvertrag gekündigt oder aus anderen Gründen beendet worden ist;
- die eingesetzte Hard- oder Software Sicherheitsmängel aufweist, die ernste Risiken für die erlaubten Anwendungen während der Zertifikatlaufzeit darstellen;
- eine TCI gemäss den vertraglichen Vereinbarungen nicht erreichbar ist;
- die den angewendeten Verfahren zugrunde liegenden Algorithmen gebrochen wurden oder wenn Gründe vorliegen, die annehmen lassen, dass die den angewendeten Verfahren zugrunde liegenden Algorithmen gebrochen wurden;
- die eindeutige Zuordnung des Schlüsselpaars zum Endanwender nicht mehr gegeben ist;
- eine gesetzliche Pflicht zum Widerruf besteht.

Widerrufe enthalten eine Angabe des Zeitpunkts des Widerrufs und den Widerrufsgrund. Alle Widerrufe werden in der vom ZDA betriebenen Zertifikatsdatenbank registriert. Diese Datenbank ist auch die Grundlage für den zur Verfügung gestellten OCSP Dienst. Zertifikate

können nicht rückwirkend widerrufen werden. Ein Widerruf kann nicht rückgängig gemacht werden.

Widerrufsberechtigte müssen sich gemäss Abschnitt *3.4. Identifizierung und Authentifizierung bei Stellung eines Widerrufsverlangens* authentifizieren.

4.9.2. Widerrufsberechtigte

Zum Widerruf eines Zertifikates ist grundsätzlich nur der Zertifikatsinhaber, der ZDA und widerrufsberechtigte Dritte berechtigt. Darüber hinaus kann die zuständige Behörde einen Zertifikatswiderruf der ZDA-Zertifikate und der Endnutzer-Zertifikate veranlassen.

4.9.3. Verfahren zur Stellung eines Widerrufsverlangens

Die Authentifizierung der Widerrufsberechtigten erfolgt gemäss Abschnitt *3.4. Identifizierung und Authentifizierung bei Stellung eines Widerrufsverlangens*.

Der Zertifikatsinhaber kann sein Zertifikat über die Website der SIGN8 AG widerrufen lassen.

Das Formular wird über https://signing.sign8.eu/revoke bereitgestellt.

Der Widerrufsberechtigte gemäss Abschnitt *3.4. Identifizierung und Authentifizierung bei Stellung eines Widerrufsverlangens* authentifiziert und nach dem erfolgreichen Widerruf seines Zertifikates informiert.

Der Widerruf eines Zertifikates ist irreversibel.

4.9.4. Fristen für ein Widerrufsverlangen

Zertifikatsinhaber haben Zertifikate unverzüglich widerrufen zu lassen, wenn und sobald Gründe für einen Widerruf vorliegen.

4.9.5. Zeitspanne für die Bearbeitung des Widerrufsverlangen

Eintreffende Widerrufsanträge werden nach erfolgreicher Authentifizierung unverzüglich bearbeitet und innerhalb von 24 Stunden umgesetzt. Sollte die Bearbeitung im Ausnahmefall nicht innerhalb von 24 Stunden umgesetzt werden, werden verantwortliche Mitarbeiter umgehend benachrichtigt und der resultierende Prozess protokolliert.

Widerrufe sind nach Durchführung unverzüglich, jedoch spätestens nach 15 Minuten, über OCSP abrufbar.

4.9.6. Methoden zum Prüfen von Widerrufsinformationen

Widerrufsinformationen können über den OCSP-Responder abgefragt werden. Die Adresse des Dienstes ist Teil des Zertifikats.

4.9.7. Häufigkeit der Veröffentlichung von Widerrufslisten

Es werden keine Widerrufslisten für Zertifikate zur Verfügung gestellt.

4.9.8. Maximale Latenzzeit für Widerrufslisten

Es werden keine Widerrufslisten für Zertifikate zur Verfügung gestellt.

4.9.9. Online-Verfügbarkeit von Widerrufsinformationen

Widerrufsinformationen können online über den OCSP-Responder abgefragt werden. Die Adresse des Dienstes ist Teil des Zertifikats. Der Zertifikatsstatus kann mindestens elf Jahre nach Ablauf der Gültigkeit über den Statusabfragedienst abgerufen werden.

4.9.10. Notwendigkeit zur Online-Prüfung von Widerrufsinformationen

Um einem Zertifikat vertrauen zu können, muss die Gültigkeit des Zertifikats über den Statusabfragedienst (OCSP) bestätigt werden.

4.9.11. Andere Formen zur Anzeige von Widerrufsinformationen

Keine Angaben.

4.9.12. Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Wenn ein privater Schlüssel kompromittiert wurde, so muss dies dem ZDA unverzüglich mitgeteilt werden. Das dazugehörige Zertifikat wird widerrufen und der private Schlüssel muss (sofern technisch möglich) vernichtet werden.

4.9.13. Suspendierung des Zertifikats

Die Suspendierung von Zertifikaten ist nicht möglich.

4.10. Statusabfragedienst

Statusabfragen erfolgen über den OCSP-Responder. Der Statusabfragedienst ist über das Protokoll OCSP nach RFC 6960 verfügbar. Die Adresse des Dienstes ist Teil des Zertifikats und 24 Stunden an sieben Tagen die Woche verfügbar. Der Statusabfragedienst ist hochverfügbar, um einen Ausfall zu verhindern werden mehrere Instanzen des OCSP betrieben. Der OCSP ist ortsunabhängig redundant aufgebaut. Der ZDA wird Störungen des Statusabfragediensts im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten umgehend beseitigen.

Die Systemzeit des OCSP-Responder wird stetig gegen die offizielle Zeit synchronisiert und es wird eine angemessene mit der UTC synchronisierte Zeitquelle verwendet.

4.11. Beendigung des Zertifizierungsdienstes

Die Verträge können von dem ZDA und dem Zertifikatsinhaber gemäss der zwischen Ihnen geschlossenen vertraglichen Vereinbarungen gekündigt werden. Andererseits endet die Gültigkeit des Zertifikates mit dem im Zertifikat vermerkten Termin. Die durch den ZDA ausgestellten Endanwender-Zertifikate sind höchstens fünf Jahre gültig.

Der ZDA verfügt über einen fortlaufend aktualisierten Beendigungsplan, in welchem Einzelheiten für den Fall der Einstellung der Tätigkeit niedergelegt sind.

Der ZDA benachrichtigt Endanwender und Dritte, einschliesslich Relying Parties und der zuständigen Aufsichtsbehörde und ggf. den fortführenden ZDA, rechtzeitig, mindestens aber zwei Monate vorher, über die Einstellung der Zertifizierungsdienste.

Der ZDA widerruft bei Übergabe an die Aufsichtsbehörde alle noch gültigen Zertifikate zum Zeitpunkt der Beendigung des Zertifizierungsdienstes. Die ausgegebenen Zertifikate sowie deren Statusinformationen werden in diesem Fall in die von der entsprechenden Aufsichtsbehörde geschaffene Vertrauensinfrastruktur, oder ggf. in die Vertrauensinfrastruktur des fortführenden ZDA, überführt. Alle privaten Schlüssel und deren Backups der betroffenen CAs werden unwiderruflich zerstört, sodass sichergestellt wird, dass eine weitere Verwendung ausgeschlossen ist.

4.12. Schlüsselhinterlegung und -wiederherstellung

Private Schlüssel werden beim qualifizierten und geregelten Fernsignatur- und Fernsiegeldienst treuhänderisch vom ZDA verwaltet. Der private Schlüssel wird sicher verwaltet. Es ist über den ZDA durch technische- und organisatorische Massnahmen sichergestellt, dass ausschliesslich der Endanwender Zugriff auf den privaten Schlüssel seines Zertifikats hat und diesen nutzen kann. Sobald das zu dem privaten Schlüssel zugehörige Zertifikat abläuft oder widerrufen wird, wird der private Schlüssel gelöscht und kann nicht wiederhergestellt werden.

In allen anderen Fällen werden keine Hinterlegung und Wiederherstellung von privaten Schlüsseln angeboten.

5. Nicht-technische Sicherheitsmassnahmen

5.1. Bauliche Sicherheitsmassnahmen

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.2. Verfahrensvorschriften

5.2.1. Rollenkonzept

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.2.2. Mehr-Augen-Prinzip

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.2.3. Sonstige Dienstanweisung

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.2.4. Standards und Kontrollen für kryptographische Module

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.3. Personalkonzept

5.3.1. Qualifikation, Erfahrung und Zuverlässigkeit des Personals

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.3.2. Sicherheitsüberprüfung

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.3.3. Schulungen und Weiterbildungen

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.3.4. Häufigkeit von Job-Rotation

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.3.5. Anforderungen an externes Personal

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.3.6. Sanktionen bei unerlaubten Handlungen

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.3.7. Dokumentation

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.4. Protokollierung von Überwachungsmassnahmen

5.4.1. Überwachung des Zutritts

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.4.2. Überwachung von organisatorischen Massnahmen

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.4.3. Art der aufgezeichneten Ereignisse

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.4.3.1. CA-Schlüsselpaare und CA-Systeme

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.4.3.2. EE- und CA-Zertifikate

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.4.3.3. Sonstige sicherheitsrelevante Ereignisse

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.5. Archivierung von Unterlagen

5.5.1. Arten von Unterlagen

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.5.2. Aufbewahrungszeiten

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.5.3. Archivsicherheit

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.5.4. Datensicherung des Archivs

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.6. Umstellung des Schlüssels (key changeover)

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.7. Notfallkonzept

5.7.1. Behandlung von Vorfällen

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.7.2. Wiederherstellung von IT-Systemen

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.7.3. Wiederherstellung nach Kompromittierung von privaten CA-Schlüsseln

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.7.4. Weiterführung des Betriebs nach Kompromittierung oder Katastrophenfall

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.7.5. Regelmässige Kontrolle

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

5.8. Beendigung des Zertifizierungsbetriebs

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6. Technische Sicherheitsmassnahmen

6.1. Erzeugung und Installation von Schlüsselpaaren

6.1.1. Erzeugung von Schlüsselpaaren

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.1.2. Auslieferung der privaten Schlüssel für Zertifikatsteilnehmer

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.1.3. Auslieferung der öffentlichen Schlüssel an die CA

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.1.4. Auslieferung der öffentlichen CA-Schlüssel

Die CA-Zertifikate, welche die dazugehörigen öffentlichen CA-Schlüssel beinhalten, werden in der Liste der anerkannten Anbieterinnen von Zertifizierungsdiensten veröffentlicht, welche durch die zuständige Aufsichtsbehörde verwaltet wird. Darüber hinaus werden alle CA-Zertifikate nach ihrer Erstellung auf der Website des ZDA veröffentlicht.

6.1.5. Schlüssellängen

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

Ausserdem entsprechen die Parameter den Anforderungen den TAV Kapitel 2.3.3.

6.1.6. Schlüsselparameter und Qualitätskontrolle der Parameter

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.1.7. Schlüsselverwendung

Alle Zertifizierungsdienste der SIGN8 benutzen für den Signaturvorgang dieselben QSCDs, die auch für die Generierung der Signierschlüssel benutzt werden. Die Trennung der Benutzungskontrolle über die Schlüssel ist sichergestellt und der Zugriff auf die, sowie die Benutzung der Schlüssel werden durch angemessene Zugriffskontrollen geschützt. Der ZDA stellt sicher, dass ein Zertifikat gültig ist, bevor ein privater Schlüssel verwendet wird. Die Verwendung eines Signierschlüssels ist nur innerhalb der QSCDs möglich.

Die CA-Schlüssel und Zeitstempelschlüssel werden ausschliesslich zum Signieren von Endanwenderzertifikaten verwendet, die OCSP-Schlüssel zum Signieren der OCSP-Anfragen. Die CA- und OCSP-Schlüssel werden in einer sicheren Umgebung eingesetzt (vergleiche Abschnitt *5.1. Bauliche Sicherheitsmassnahmen*). Die Schlüsselverwendung für Teilnehmerzertifikate ist Teil des X.509 Zertifikats und darf ausschliesslich für qualifizierte und geregelte Signaturen und Siegel verwendet werden.

Gemäss Kapitel 2.2.3 TAV wird eine elektronische Signatur oder Siegel unter Verwendung der zugehörigen elektronischen Erstellungsdaten generiert, die der Unterzeichner mit einem hohen Mass an Vertrauen unter seiner alleinigen Kontrolle verwenden kann. Der Signatur- oder Siegelvorgang muss durch den Unterzeichner zugestimmt werden. Die Zustimmung wird durch die Eingabe oder durch die Bestätigung des Authentifizierungsmittel angenommen. SIGN8 geht somit davon aus, dass der private Schlüssel eines Unterzeichners nur unter seiner Zustimmung verwendet wird. Eine elektronische Signatur bzw. Siegel ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Private Schlüssel werden nicht zur Authentifizierung verwendet.

6.2. Schutz privater Schlüssel und technische Kontrollen kryptographischer Module

6.2.1. Standards und Sicherheitsmassnahmen

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.2.2. Schlüsselaktivierung

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.2.3. Schlüsselwiederherstellung

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.2.4. Schlüsselbackup

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.2.5. Schlüsselarchivierung

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.2.6. Schlüsseltransfer

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.2.7. Schlüsselspeicherung

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.2.8. Aktivierung privater Schlüssel

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.2.9. Deaktivierung privater Schlüssel

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.2.10. Zerstörung privater Schlüssel

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.2.11. Beschreibung der kryptografischen Module

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.3. Weitere Aspekte der Verwaltung des Schlüsselpaars

6.3.1. Archivierung der öffentlichen Schlüssel

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.3.2. Gültigkeitsdauer von Schlüssel und Zertifikaten

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.4. Aktivierungsdaten

6.4.1. Erzeugung und Installation von Aktivierungsdaten

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.4.2. Schutz von Aktivierungsdaten

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.4.3. Weitere Aspekte der Aktivierungsdaten

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.5. Computer-Sicherheitsmassnahmen

6.5.1. Spezifische technische Sicherheitsanforderungen an Computer-Systeme

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.5.2. Bewertung der Computersicherheit

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.6. Technische Kontrolle während des Lebenszyklus

6.6.1. Sicherheitsmassnahmen beim Aufbau, der Entwicklung und Erweiterung der IT-Systeme und Softwarekomponenten

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.6.2. Sicherheitsmassnahmen beim Computermanagement

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.6.3. Sicherheitsmassnahmen beim Betrieb

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.7. Netzwerksicherheit

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.8. Zeitstempel

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

6.9. API-Sicherheit

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

7. Profile von Zertifikaten, Widerrufslisten und OCSP

Qualifizierte und geregelte Zertifikate für elektronische Signaturen und Siegel erfüllen die im Kapitel 2.3 der TAV (SR 943.032.1) festgelegten Anforderungen und unterliegen keinen weiteren zwingenden Anforderungen. Die Zertifikatsprofile entsprechen den Vorgaben nach RFC 5280 und werden im Format X.509v3 ausgegeben. Qualifizierte und geregelte Zertifikate für elektronische Signaturen und Siegel können zusätzliche spezifische Attribute enthalten, die nicht obligatorisch sind. Kritische Erweiterungen enthalten den Zusatz „kritisch“.

Nicht obligatorische Attribute dürfen nicht und beeinträchtigen nicht die Interoperabilität und Anerkennung qualifizierter und geregelter elektronischer Signaturen und Siegel.

Nicht obligatorische Attribute dürfen nicht und beeinträchtigen nicht die Interoperabilität und Anerkennung qualifizierter elektronischer Signaturen und Siegel.

Ergänzende Erweiterungen können aufgenommen werden, müssen dabei alle von ETSI EN 319 412-5 referenzierte RFCs entsprechen oder in einem referenzierten Dokument beschrieben sein.

Semantik Identifizierungsattribute können inkludiert werden, müssen den Spezifikationen in ETSI EN 319 412-1 und den dort referenzierten Normen und RFCs entsprechen.

Die Zertifikatsprofile sind im [Cert Profile] detailliert beschrieben.

7.1 OIDs der genutzten Algorithmen

Die folgenden Signatur- und Hash-Algorithmen werden derzeit in Endbenutzer- und CA-Zertifikaten sowie Signaturen verwendet:

OID	Beschreibung
2.16.840.1.101.3.4.2.1	SHA256
2.16.840.1.101.3.4.2.3	SHA512
1.2.840.10045.2.1	eccEncryption
1.2.840.10045.4.3.2	Ecdsa-with-SHA256
1.2.840.10045.4.3.4	Ecdsa-with-SHA521
1.2.840.113549.1.1.1	rsaEncryption

7.2 Certificate Revocation List Profile (CRL)

Es werden keine Widerrufslisten von SIGN8 angeboten.

7.3 Status Query Service Profile (OCSP)

Ein OCSP-Responder wird gemäss RFC 6960 zur Abfrage des Status von Zertifikaten betrieben. Das OCSP-Zertifikat enthält die Erweiterung „OCSPnoCheck“ und verwendet nicht die AIA-Erweiterung „id-ad-ocsp“ accessMethod.

Der OCSP-Responder des ZDA liefert einem anfragenden Dritten Informationen über die Gültigkeit eines Zertifikats zu einem bestimmten Zeitpunkt. Folgende Status werden zurückgegeben:

- good - Das Zertifikat ist im Verzeichnisdienst vorhanden und nicht widerrufen,
- unknown - Der OCSP kann keine genauen Informationen über den Status des Zertifikats liefern.
- revoked - Das Zertifikat sollte abgelehnt werden.

8. Konformitätsprüfung

SIGN8 ermöglicht der zuständigen Aufsichtsstelle und einer anerkannten Konformitätsbewertungsstelle die Überprüfung der Konformität nach den folgenden Vorgaben:

- ZertES (Stand am 1. Januar 2020)
- VZertES (Stand am 1. November 2025)
- TAV SR 943.032.1 (Stand am 1. November 2025)
- ETSI EN 319 401 V3.2.1 (2025-11)
- ETSI EN 319 411-1 V1.4.1 (2023-10)
- ETSI EN 319 411-2 V2.5.1 (2021-05)
- ETSI EN 319 412-1 V1.5.1 (2023-09)
- ETSI EN 319 412-2 V2.3.1 (2023-09)
- ETSI EN 319 412-3 V1.3.1 (2023-09)
- ETSI EN 319 412-5 V2.4.1 (2023-09)
- ETSI EN 319 421 V1.2.1 (2023-05)
- ETSI EN 319 422 V1.1.1 (2016-03)
- EN 419241-1:2018-09 (SCAL 1 und SCAL 2)
- ETSI TS 119 431-1 V1.3.1 (2024-12)

Im Rahmen der Audits wird, neben der Dokumentation (Sicherheitskonzept, CPS sowie weitere interne Dokumente), die Umsetzung der Prozesse und Einhaltung der Vorgaben überprüft.

8.1. Intervall oder Gründe von Prüfungen

Die SIGN8 unterliegt einer kontinuierlichen Konformitätsprüfung als qualifizierter ZDA, deren rechtliche Basis im ZertES verankert ist.

Die jährliche Überprüfung der erbrachten qualifizierten und geregelten Zertifizierungsdienste durch eine akkreditierte Konformitätsbewertungsstelle ist obligatorisch. Dies dient dem Nachweis, dass alle Anforderungen des ZertES, der VZertES und der TAV erfüllt werden.

Die Aufsichtsstelle kann jederzeit auf Kosten der SIGN8 ein Audit durchführen oder eine Konformitätsbewertungsstelle um eine Konformitätsbewertung der SIGN8 ersuchen, um zu bestätigen, dass sie und die von ihnen erbrachten qualifizierten und geregelten Zertifizierungsdienste die Anforderungen des ZertES erfüllen.

SIGN8 informiert die Aufsichtsstelle mindestens einen Monat vor der geplanten Überprüfung und erlaubt diesen auf Anfrage als Beobachter teilzunehmen. Der entsprechende Konformitätsbewertungsbericht wird der Aufsichtstelle innerhalb von drei Arbeitstagen nach Empfang vorgelegt.

Der Zugang zu den Informationen ist im Abschnitt *2.4. Zugang zu den Informationen* beschrieben.

8.2. Identität/Qualifikation des Prüfers

Die ZDA-spezifischen Konformitätsprüfungen werden von qualifizierten Dritten durchgeführt, die Erfahrung in den Bereichen PKI-Technologie, Sicherheits-Auditing und Verfahren sowie Hilfsmittel der Informationssicherheit vorweisen können. Die Identität des Prüfers ist dem jeweiligen Konformitätsbewertungsbericht zu entnehmen.

8.3. Beziehung des Prüfers zur prüfenden Stelle

Beim Prüfer für die Konformitätsprüfung handelt es sich um einen unabhängigen und qualifizierten Auditor.

8.4. Abgedeckte Bereiche der Prüfung

Zielsetzung der Überprüfung ist die Umsetzung der gesamten zum Zertifizierungsdienst gehörenden Dokumentation sowie die Umsetzung der beschriebenen Prozesse. Es sind alle Prozesse zu prüfen, die mit der Lebenszyklusverwaltung von Zertifikaten in Verbindung stehen:

- Identitätsprüfung der Endanwender,
- Zertifikatsbeantragungsverfahren,
- Bearbeitung von Zertifikatsanträgen,
- Zertifikatswiederrufe,
- Zertifikatssperrungen,
- Zutrittsschutz,
- Berechtigungs- und Rollenkonzept,
- Einbruchshemmende Massnahmen,
- Personal.

8.5. Massnahmen zur Mängelbeseitigung

Werden Mängel festgestellt, werden geeignete Massnahmen zu deren Beseitigung eingeleitet. Falls die Sicherheit des Betriebs der Zertifizierungsdienste gefährdet ist, wird gegebenenfalls der Betrieb bis zur Beseitigung der Mängel eingestellt.

Erfüllt SIGN8 eine der in dem ZertES, der VZertES oder den TAV festgelegten Anforderungen nicht, so fordert die Aufsichtsstelle SIGN8 auf, gegebenenfalls innerhalb einer bestimmten Frist Abhilfe zu schaffen. Sorgt SIGN8 nicht innerhalb der von der Aufsichtsstelle gesetzten

Frist für Abhilfe, entzieht die Aufsichtsstelle der SIGN8 oder den erbrachten Diensten den qualifizierten Status, wenn dies insbesondere aufgrund des Umfangs, der Dauer und der Folgen des Versäumnisses gerechtfertigt ist.

8.6. Veröffentlichung von Ergebnissen

Die Ergebnisse des Audits bzw. der Mängelbeseitigung werden nicht veröffentlicht.

8.7. Nutzung des Vertrauenssiegel

Keine Angaben.

9. Sonstige geschäftliche und rechtliche Regelungen

9.1. Preise

9.1.1. Preise für die Ausgabe von Zertifikaten

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

9.1.2. Gebühren für den Zugriff auf Zertifikate

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

9.1.3. Gebühren für den Widerruf von Zertifikaten oder den Erhalt von Statusinformationen

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

9.1.4. Gebühren für andere Dienstleistungen

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

9.1.5. Kostenrückerstattungen

Die entsprechenden Einzelheiten sind in der [CPS eIDAS] beschrieben.

9.2. Finanzielle Verantwortung

Der ZDA verfügt über die notwendigen Ressourcen sowie die finanzielle Stabilität, um den Betrieb der Zertifizierungsdienste ordnungsgemäss durchzuführen.

Der ZDA verpflichtet sich zur Haftung gegenüber Zertifikatsinhabern und Dritten für Schäden aus Pflichtverletzungen gemäss Art. 17 ZertES, trägt dafür die Beweislast und schliesst lediglich die Haftung für die Überschreitung von Nutzungsbeschränkungen aus.

Zur Deckung von Haftungsansprüchen hat der ZDA eine Haftpflichtversicherung abgeschlossen. Die Höhe der Versicherungssumme entspricht den Anforderungen von Art. 17 Absatz 1 ZertES und Artikel 2 VZertES und gewährleistet somit eine ausreichende Deckung.

9.3. Vertraulichkeit von Geschäftsdaten

9.3.1. Definition von vertraulichen Geschäftsdaten

Die Vertraulichkeit von Informationen ist bereits durch geltendes Recht definiert.

9.3.2. Geschäftsdaten die nicht vertraulich behandelt werden

Als öffentlich gelten alle Informationen in ausgestellten und veröffentlichten Zertifikaten sowie die unter Abschnitt *2.2. Veröffentlichung von Informationen zu Zertifikaten* genannten Daten.

9.3.3. Zuständigkeiten für den Schutz vertraulicher Geschäftsdaten

Der ZDA ist dazu verpflichtet vertrauliche Geschäftsdaten durch entsprechende technische und organisatorische Massnahmen gegen Preisgabe und Ausspähung zu schützen, und hat zu unterlassen, dass diese Daten zweckentfremdet genutzt werden oder diese Daten Drittpersonen offengelegt werden, soweit eine solche Verpflichtung nicht gegen das Gesetz verstösst. Im Rahmen der organisatorischen Massnahmen werden, die vom ZDA eingesetzten Mitarbeiter in dem gesetzlich zulässigen Rahmen zur Geheimhaltung der vertraulichen Daten verpflichtet.

9.4. Schutz von Personendaten

Der ZDA beachtet die gesetzlichen Bestimmungen zum Datenschutz.

Zur Bereitstellung von Zertifizierungsdiensten setzt SIGN8 AG die in Deutschland ansässige SIGN8 GmbH ein, bei der auch die Ausstellung der digitalen Zertifikate technisch erfolgt.

Der Dienst ist folglich als Auftragsbearbeitung in Deutschland durch die SIGN8 GmbH zu qualifizieren, die weisungsgebunden für SIGN8 AG tätig wird. SIGN8 AG hat die hierfür datenschutzrechtlich notwendigen Verträge mit der SIGN8 GmbH geschlossen. Mit der Annahme der Nutzungsbedingungen der SIGN8 AG erklären sich die Unterzeichnenden hiermit einverstanden.

9.4.1. Datenschutzkonzept

Die Datenschutzerklärung kann unter folgendem Link eingesehen werden: https://sign8.ch/impressum-datenschutzerklaerung/.

9.4.2. Definition von Personendaten

Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen und nicht bereits öffentlich im Zertifikat einsehbar sind.

9.4.3. Nicht vertrauliche Daten

Alle Informationen und Daten, die in den von dem ZDA ausgegebenen Zertifikaten und in den in Abschnitt *2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen* genannten Dokumenten explizit oder implizit enthalten sind oder daraus abgeleitet werden können, werden als nicht vertrauliche Daten behandelt.

9.4.4. Verantwortung für den Schutz Personendaten

Der ZDA gewährleistet die Einhaltung des Datenschutzes.

Der Datenschutzbeauftragte des ZDA achtet auf die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz. Er erarbeitet Datenschutzrichtlinien, steht als

Ansprechpartner in Datenschutzfragen zur Verfügung und verpflichtet die Mitarbeiter des ZDA oder mit dem ZDA in vertraglicher Verbindung stehende Dritte mit Zugriff auf Personendaten zur Beachtung der Datenschutzrichtlinien.

9.4.5. Hinweis und Einwilligung zur Nutzung von Personendaten

Bei der Antragsstellung wird der Zertifikatsinhaber darüber informiert, welche Personendaten auf dem Zertifikat enthalten sein werden.

Bei der Antragsstellung werden Personendaten des Zertifikatnehmers im Rahmen des Identifikationsverfahrens erhoben und verarbeitet. Der Zertifikatnehmer stimmt im Rahmen der Antragstellung der Nutzung seiner Personendaten zu.

9.4.6. Erteilung von Auskünften im Rahmen von Gerichts- oder Verwaltungsverfahren

Die Auskunfts- und Mitwirkungspflichten des ZDA gegenüber Gerichten und anderen Behörden bleiben von den Regelungen dieses CPS und von konkreten vertraglichen Regelungen unberührt. Auskünfte über vertrauliche oder Personendaten werden den ermittelnden Behörden herausgegeben, sofern ein Gerichtsbeschluss vorliegt oder sonstige gesetzlichen Bestimmungen eine Herausgabe erfordern. Etwaige Herausgaben werden vom ZDA dokumentiert und für 12 (in Worten: zwölf) Monate archiviert.

9.4.7. Andere Bedingungen für Auskünfte

Auskünfte anderer Art als unter Abschnitt *9.4.6. Erteilung von Auskünften im Rahmen von Gerichts- oder Verwaltungsverfahren* beschrieben werden nicht erteilt.

9.5 Urheberrechte

9.5.1 ZDA

Bestand und Inhalt von Urheber- und sonstigen Immaterialgüterrechten richten sich nach den allgemeinen gesetzlichen Vorschriften.

9.5.2. Zertifikatsnehmer

Der Zertifikatsnehmer verpflichtet sich zur Einhaltung geistiger Eigentumsrechte in den Antrags- und Zertifikatsdaten.

9.6. Zusicherungen, Garantien und Gewährleistung

Dieses Zertifikationskonzept enthält keine Zusicherungen, Garantien oder Gewährleistungen seitens des ZDA.

Der ZDA stellt sicher, dass die in dem CPS beschriebenen Verfahren eingehalten werden.

Im Verhältnis zu Zertifikatsinhabern, Relying Parties sowie allen anderen Personen sind ausschliesslich die entsprechenden Regelungen in den AGB bzw. der jeweiligen einzelvertraglichen Vereinbarung sowie die gesetzlichen Bestimmungen massgeblich.

9.7. Haftungsausschluss

Ein Haftungsausschluss ist in den AGB oder einzelvertraglich geregelt.

9.8. Haftungsbeschränkung

Es gelten die etwaigen jeweiligen Vereinbarungen und die entsprechenden AGB.

9.9. Schadensersatz

Es gelten die etwaigen jeweiligen Vereinbarungen und die entsprechenden AGB.

9.10. Laufzeit und Beendigung

SIGN8 unterrichtet die Aufsichtsstelle mindestens einen Monat vor einer Änderung bei der Erbringung ihrer qualifizierten Zertifizierungsdienste oder mindestens drei Monate im Falle einer beabsichtigten Einstellung dieser Tätigkeiten.

9.10.1. Gültigkeitsdauer des CPS

Dieses CPS gilt ab dem Zeitpunkt der Veröffentlichung und bleibt wirksam bis zum Ablauf des letzten, unter diesem CPS ausgestellten Zertifikats. Es gilt jeweils die Version der CPS, die zum Zeitpunkt der Antragsstellung veröffentlicht ist.

9.10.2. Beendigung der Dienste

Für den Fall, dass der ZDA den Betrieb einstellt, liegt ein Beendigungsplan vor, der regelmässig auf Aktualität überprüft wird.

9.10.3. Auswirkung der Beendigung

Ist absehbar, dass der komplette Betrieb des ZDA oder Teile davon eingestellt werden, so wird diese Beendigung gemäss des Beendigungsplans des ZDA durchgeführt. Der ZDA hat zu prüfen, ob eine Übernahme des jeweiligen Dienstes durch einen anderen qualifizierten und geregelten Zertifizierungsdiensteanbieter möglich ist. In dem Fall werden alle vom ZDA ausgegebenen Zertifikate und Widerrufsinformationen für den zu beendenden Dienst in elektronischer Form an den neuen Zertifizierungsdiensteanbieter übergeben.

Ist eine Übernahme des Dienstes durch einen ZDA ausgeschlossen, so werden alle vom ZDA ausgegebenen Zertifikate und Widerrufsinformationen für den zu beendenden Dienst in elektronischer Form an die BAKOM zur Übernahme in die Vertrauensinfrastruktur übergeben. Alle zu diesem Dienst zugehörigen Endanwenderzertifikate werden vor der Übergabe an die BAKOM widerrufen, der private CA-Schlüssel wird vernichtet, so dass keine neuen Zertifikate

ausgestellt werden können. Gegebenenfalls sind weitere Schritte mit der jeweiligen Aufsichtsbehörde abzustimmen.

In jedem Fall wird der Endanwender über diese Beendigung, mithilfe der aus der Registrierung hinterlegten Kontaktdaten, informiert.

9.11. Mitteilungen an und Kommunikation mit Teilnehmern

Mitteilungen des ZDA an Zertifikatnehmer werden an die letzte in den Unterlagen des ZDA verzeichnete Anschrift oder der entsprechenden E-Mail-Adresse aus dem Antrag versendet.

9.12. Änderung des Zertifizierungskonzeptes

9.12.1. Verfahren für Änderungen

Veränderungen und Nachträge zu diesem CPS werden in diesem Dokument eingearbeitet und als eine neue Version veröffentlicht. Editorische Änderungen werden markiert.

9.12.2. Benachrichtigungsverfahren und -fristen

Veränderungen und Nachträge zu diesem CPS, die Kunden oder Drittbeteiligte betreffen, werden veröffentlicht und kommuniziert nach Abschnitt *2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen*.

9.12.3. Bedingungen für OID-Änderungen

Keine Angaben

9.13. Streitschlichtungsverfahren

Beschwerden können schriftlich bei SIGN8 AG c/o SWISS COMPANY AG, Bahnhofstrasse 21, 6300 Zug oder via E-Mail (info@sign8.ch) eingereicht werden.

9.14. Anwendbares Recht

Dieses CPS unterliegt dem materiellen Recht der Schweiz unter Ausschluss seiner kollisionsrechtlichen Bestimmungen sowie des CISG (UN-Kaufrechts).

9.15. Einhaltung geltenden Rechts

Der jeweilige Zertifikatsinhaber ist dafür verantwortlich, dass die von dem ZDA ausgegebenen Zertifikate im Einklang mit den gesetzlichen Bestimmungen verwendet werden.

9.16. Sonstige Bestimmungen

9.16.1. Barrierefreiheit

Die entsprechenden Einzelheiten sind im [CPS eIDAS] beschrieben.

9.16.2. Nichtdiskriminierungsklausel

Die entsprechenden Einzelheiten sind im [CPS eIDAS] beschrieben.

9.16.3. Vollständigkeitserklärung

Folgende Dokumente sind Gegenstand der geltenden Vereinbarungen an denen PKI-Teilnehmer beteiligt sind:

- Vertrags- und Antragsunterlagen,
- die zum Zeitpunkt der Antragsstellung gültigen Allgemeine Geschäftsbestimmungen (AGB) bzw. die ggf. wirksam einbezogene Fassung derselben,
- die zum Zeitpunkt der Antragsstellung gültige CPS,
- Das Service Level Agreement.

9.16.4. Abgrenzung

Keine Abgrenzung, solange der Nutzer den AGB zustimmt.

9.16.5. Salvatorische Klausel

Sind oder werden einzelne Bestimmungen dieses Vertrags unwirksam, so wird dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Die Vertragspartner werden in diesem Fall die ungültige Bestimmung durch eine andere ersetzen, die dem wirtschaftlichen Zweck der weggefallenen Regelung in zulässiger Weise am nächsten kommt.

9.16.6. Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

Es gelten die etwaigen jeweiligen Vereinbarungen und die entsprechenden AGB.

9.16.7. Höhere Gewalt

Es gelten die etwaigen jeweiligen Vereinbarungen und die entsprechenden AGB.

9.17. Andere Bestimmungen

Es erfolgen keine weiteren Angaben.