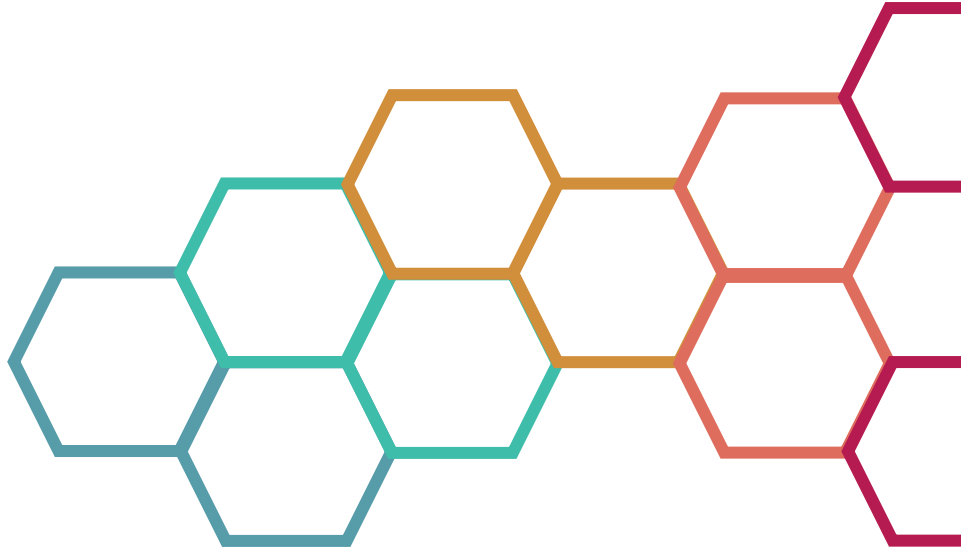




SIGN8 GmbH
Fürstenrieder Str. 5
80687 München

T: +49 (0)89 / 2153 7472 000
info@sign8.eu
www.sign8.eu

Certificate Practice Statement der SIGN8 GmbH



Version: 1.6
Datum: 15.01.2026

Unterschrift: _____

(Geschäftsführer SIGN8 GmbH)

Dokumentationshistorie

Version	Anmerkung	Datum
1.1	Erstellung des Dokuments im Rahmen der Prüfung der Einhaltung der Vorgaben der Verordnung (EU) Nr. 910/2014 des europäischen Parlamentes und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung) durch eine akkreditierte Konformitätsbewertungsstelle.	25.01.2023
1.2	Dokument erweitert um weitere Identifizierungsoptionen und lokale Zertifikate. Einarbeitung weiterer textueller Anpassungen.	26.05.2023
1.3	Dokument ergänzt um weitere Identifizierungsoption und Erweiterung Zertifikatsantragsprozess	03.11.2023
1.4	Erweiterung des Dokuments im Rahmen der Prüfung der Einhaltung der Vorgaben der Verordnung (EU) Nr. 2024/1183 des europäischen Parlamentes und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 hinsichtlich der Schaffung eines europäischen Rahmens für die digitale Identität	10.09.2024
1.5	Erweiterung des Dokuments zur Erfüllung weiterer ETSI Anforderungen	25.11.2024
1.6	Anpassung Widerrufsgründe	15.01.2026

Referenzierte Dokumente

Kürzel	Beschreibung
[Cert Profile eIDAS]	Addendum zum CPS: Profile der Zertifikate und Online Statusabfragen (OCSP)

Inhalt

1. Einleitung	10
1.1. Überblick	10
1.1.1. Über dieses Dokument	10
1.1.2. Eigenschaften der PKI von SIGN8	11
1.2. Name und Kennzeichnung des Dokuments	12
1.3. PKI-Teilnehmer	12
1.3.1. Zertifizierungsstelle (CA)	12
1.3.2. Registrierungsstellen (RA)	12
1.3.3. Zertifikatsinhaber und Endanwender	12
1.3.4. Zertifikatsprüfer (Relying Party)	13
1.3.5. Andere Teilnehmer	13
1.3.6. Lizenznehmer	13
1.3.7. Unterzeichner	13
1.4. Verwendung von Zertifikaten	13
1.4.1. Gültigkeitsmodell	14
1.4.2. Verwendung von Dienstzertifikaten	14
1.5. Verwaltung der Konzepte	14
1.6. Definitionen und Abkürzungen	15
1.7. Übertragung von Aufgaben an Dritte	18
1.8. Ansprechpartner	19
2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen	20
2.1. Verzeichnisse	20
2.2. Veröffentlichung von Informationen zu Zertifikaten	20
2.3. Zeitpunkt und Häufigkeit von Veröffentlichungen	20
2.4. Zugang zu den Informationen	21
3. Identifizierung und Authentifizierung	22
3.1. Namensregeln	22
3.1.1. Arten von Namen	22
3.1.2. Aussagekraft von Namen	22
3.1.3. Pseudonyme	22
3.1.4. Regeln für die Interpretation verschiedener Namensformen	22

3.1.5. Eindeutigkeit von Namen	22
3.1.6. Anerkennung, Authentifizierung und die Rolle von Markennamen	22
3.1.7. Password-Policy	22
3.1.8. Test-Zertifikate	23
3.2. Identifizierung der Zertifikatsinhaber	23
3.2.1. Nachweis über den Besitz des privaten Schlüssels.....	23
3.2.2. Identifizierung und Authentifizierung von Organisationen	23
3.2.3. Identifizierung und Authentifizierung natürlicher Personen.....	25
3.2.4. Ungeprüfte Angaben zum Zertifikatsnehmer	26
3.2.5. Überprüfung fremder CAs, RAs	26
3.2.6. Prüfung der Berechtigung zur Antragsstellung	26
3.2.7. Interoperabilität	26
3.3. Identifizierung und Authentifizierung bei Anträgen auf Schlüsselerneuerung (re-keying).....	26
3.4. Identifizierung und Authentifizierung bei Stellung eines Widerrufsverlangens.....	27
4. Betriebsanforderungen.....	28
4.1. Zertifikatsantrag.....	28
4.2. Verarbeitung des Zertifikatsantrags	29
4.2.1. Durchführung der Identifizierung und Authentifizierung	29
4.2.2. Annahme oder Ablehnung des Antrags	30
4.3. Ausstellung von Zertifikaten	30
4.3.1. Vorgehen der CA bei der Ausstellung des Zertifikats	30
4.3.2. Benachrichtigung des Zertifikatsinhabers über die Erstellung des Zertifikats	30
4.4. Zertifikatsübergabe.....	30
4.4.1. Verhalten bei der Zertifikatsübergabe	30
4.4.2. Veröffentlichung des Zertifikats durch den VDA.....	31
4.4.3. Benachrichtigung Dritter über die Erstellung des Zertifikats	31
4.5. Verwendung des Schlüsselpaars und des Zertifikats	31
4.5.1. Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber.....	31
4.5.2. Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsinhaber.....	31
4.6. Zertifikatserneuerung	31
4.7. Zertifikatserneuerung mit Schlüsselerneuerung	32
4.8. Zertifikatsänderung.....	32

4.9. Widerruf und Suspendierung von Zertifikaten	32
4.9.1. Bedingungen für einen Widerruf	32
4.9.2. Widerrufsberechtigte	33
4.9.3. Verfahren zur Stellung eines Widerrufsverlangens	34
4.9.4. Fristen für ein Widerrufsverlangen	34
4.9.5. Zeitspanne für die Bearbeitung des Widerrufsverlangens	34
4.9.6. Methoden zum Prüfen von Widerrufsinformationen	34
4.9.7. Häufigkeit der Veröffentlichung von Widerrufslisten	34
4.9.8. Maximale Latenzzeit für Widerrufslisten	34
4.9.9. Online-Verfügbarkeit von Widerrufsinformationen	34
4.9.10. Notwendigkeit zur Online-Prüfung von Widerrufsinformationen	35
4.9.11. Andere Formen zur Anzeige von Widerrufsinformationen	35
4.9.12. Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels	35
4.9.13. Suspendierung des Zertifikats	35
4.10. Statusabfragedienst	35
4.11. Beendigung des Zertifizierungsdienstes	35
4.12. Schlüssel hinterlegung und -wiederherstellung	36
5. Nicht-technische Sicherheitsmaßnahmen	37
5.1. Bauliche Sicherheitsmaßnahmen	37
5.2. Verfahrensvorschriften	38
5.2.1. Rollenkonzept	38
5.2.2. Mehr-Augen-Prinzip	38
5.2.3. Sonstige Dienstanweisung	38
5.2.4. Standards und Kontrollen für kryptographische Module	38
5.3. Personalkonzept	39
5.3.1. Qualifikation, Erfahrung und Zuverlässigkeit des Personals	39
5.3.2. Sicherheitsüberprüfung	39
5.3.3. Schulungen und Weiterbildungen	40
5.3.4. Häufigkeit von Job-Rotation	41
5.3.5. Anforderungen an externes Personal	41
5.3.6. Sanktionen bei unerlaubten Handlungen	41
5.3.7. Dokumentation	42
5.4. Protokollierung von Überwachungsmaßnahmen	42
5.4.1. Überwachung des Zutritts	42

5.4.2. Überwachung von organisatorischen Maßnahmen	42
5.4.3. Art der aufgezeichneten Ereignisse	42
5.5. Archivierung von Unterlagen	43
5.5.1. Arten von Unterlagen.....	43
5.5.2. Aufbewahrungszeiten	43
5.5.3. Archivsicherheit.....	44
5.5.4. Datensicherung des Archivs	44
5.6. Umstellung des Schlüssels (key changeover)	44
5.7. Notfallkonzept	44
5.7.1. Behandlung von Vorfällen.....	44
5.7.2. Wiederherstellung von IT-Systemen	45
5.7.3. Wiederherstellung nach Kompromittierung von privaten CA-Schlüsseln	45
5.7.4. Weiterführung des Betriebs nach Kompromittierung oder Katastrophenfall	46
5.7.5. Regelmäßige Kontrolle.....	46
5.8. Beendigung des Zertifizierungsbetriebs	46
5.8.1. Beendigung des Zertifizierungsbetriebs eines kreuz-zertifizierten VDAs	46
6. Technische Sicherheitsmaßnahmen.....	47
6.1. Erzeugung und Installation von Schlüsselpaaren.....	47
6.1.1. Erzeugung von Schlüsselpaaren	47
6.1.2. Auslieferung der privaten Schlüssel für Zertifikatsteilnehmer.....	47
6.1.3. Auslieferung der öffentlichen Schlüssel an die CA.....	47
6.1.4. Auslieferung der öffentlichen CA-Schlüssel.....	47
6.1.5. Schlüssellängen.....	48
6.1.6. Schlüsselparameter und Qualitätskontrolle der Parameter	48
6.1.7. Schlüsselverwendung	48
6.2. Schutz privater Schlüssel und technische Kontrollen kryptographischer Module	49
6.2.1. Standards und Sicherheitsmaßnahmen	49
6.2.2. Schlüsselaktivierung	49
6.2.3. Schlüsselwiederherstellung.....	50
6.2.4. Schlüsselbackup.....	50
6.2.5. Schlüsselarchivierung	51
6.2.6. Schlüsseltransfer.....	51
6.2.7. Schlüsselspeicherung	51
6.2.8. Aktivierung privater Schlüssel	51

6.2.9. Deaktivierung privater Schlüssel	51
6.2.10. Zerstörung privater Schlüssel	51
6.2.11. Beschreibung der kryptografischen Module	52
6.3. Weitere Aspekte der Verwaltung des Schlüsselpaars	52
6.3.1. Archivierung der öffentlichen Schlüssel	52
6.3.2. Gültigkeitsdauer von Schlüssel und Zertifikaten.....	52
6.4. Aktivierungsdaten	52
6.4.1. Erzeugung und Installation von Aktivierungsdaten.....	52
6.4.2. Schutz von Aktivierungsdaten	53
6.4.3. Weitere Aspekte der Aktivierungsdaten.....	53
6.5. Computer-Sicherheitsmaßnahmen.....	53
6.5.1. Spezifische technische Sicherheitsanforderungen an Computer-Systeme.....	53
6.5.2. Bewertung der Computersicherheit	54
6.6. Technische Kontrolle während des Lebenszyklus.....	54
6.6.1. Sicherheitsmaßnahmen beim Aufbau, der Entwicklung und Erweiterung der IT-Systeme und Softwarekomponenten.....	54
6.6.2. Sicherheitsmaßnahmen beim Computermanagement	54
6.6.3. Sicherheitsmaßnahmen beim Betrieb.....	54
6.7. Netzwerksicherheit	55
6.8. Zeitstempel.....	57
6.9. API-Sicherheit	57
7. Profile von Zertifikaten, Widerrufslisten und OCSP.....	58
7.1. Zertifikatsprofile	58
7.1.1 OIDs der genutzten Algorithmen	58
7.1.2 Certificate Revocation List Profile (CRL)	59
7.1.3 Status Query Service Profile (OCSP).....	59
8. Konformitätsprüfung	60
8.1. Intervall oder Gründe von Prüfungen	60
8.2. Identität/Qualifikation des Prüfers	60
8.3. Beziehung des Prüfers zur prüfenden Stelle	60
8.4. Abgedeckte Bereiche der Prüfung	61
8.5. Maßnahmen zur Mängelbeseitigung.....	61
8.6. Veröffentlichung von Ergebnissen.....	61
8.7. Nutzung des Vertrauenssiegel	61
9. Sonstige geschäftliche und rechtliche Regelungen	62

9.1. Preise	62
9.1.1. Preise für die Ausgabe von Zertifikaten.....	62
9.1.2. Gebühren für den Zugriff auf Zertifikate.....	62
9.1.3. Gebühren für den Widerruf von Zertifikaten oder den Erhalt von Statusinformationen.....	62
9.1.4. Gebühren für andere Dienstleistungen	62
9.1.5. Kostenrückerstattungen	62
9.2. Finanzielle Verantwortung.....	62
9.3. Vertraulichkeit von Geschäftsdaten	63
9.3.1. Definition von vertraulichen Geschäftsdaten	63
9.3.2. Geschäftsdaten die nicht vertraulich behandelt werden	63
9.3.3. Zuständigkeiten für den Schutz vertraulicher Geschäftsdaten.....	63
9.4. Schutz von personenbezogenen Daten	63
9.4.1. Datenschutzkonzept.....	63
9.4.2. Definition von personenbezogenen Daten.....	63
9.4.3. Nicht vertrauliche Daten.....	64
9.4.4. Verantwortung für den Schutz personenbezogener Daten	64
9.4.5. Hinweis und Einwilligung zur Nutzung personenbezogener Daten	64
9.4.6. Erteilung von Auskünften im Rahmen von Gerichts- oder Verwaltungsverfahren..	64
9.4.7. Andere Bedingungen für Auskünfte	64
9.5 Urheberrechte	65
9.5.1 VDA.....	65
9.5.2. Zertifikatsnehmer	65
9.6. Zusicherungen, Garantien und Gewährleistung.....	65
9.7. Haftungsausschluss	65
9.8. Haftungsbeschränkung	65
9.9. Schadensersatz.....	65
9.10. Laufzeit und Beendigung.....	65
9.10.1. Gültigkeitsdauer des CPS	65
9.10.2. Beendigung der Dienste	66
9.10.3. Auswirkung der Beendigung.....	66
9.11. Mitteilungen an und Kommunikation mit Teilnehmern.....	66
9.12. Änderung des Zertifizierungskonzeptes	66
9.12.1. Verfahren für Änderungen	66
9.12.2. Benachrichtigungsverfahren und -fristen	66

9.12.3. Bedingungen für OID-Änderungen.....	66
9.13. Streitschlichtungsverfahren	67
9.14. Anwendbares Recht.....	67
9.15. Einhaltung geltenden Rechts.....	67
9.16. Sonstige Bestimmungen	67
9.16.1. Barrierefreiheit.....	67
9.16.2. Nichtdiskriminierungsklausel	67
9.16.3. Vollständigkeitserklärung	67
9.16.4. Abgrenzung.....	68
9.16.5. Salvatorische Klausel.....	68
9.16.6. Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht).....	68
9.16.7. Höhere Gewalt	68
9.17. Andere Bestimmungen	68

1. Einleitung

1.1. Überblick

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

Der Vertrauensdiensteanbieter, im Folgenden VDA genannt, ist – auch im juristischen Sinne – die

SIGN8 GmbH
Fürstenrieder Str. 5
80687 München.

Der VDA ist qualifizierter Vertrauensdiensteanbieter i.S.d. Artikel 21 Abs. 2 der VO (EU) Nr. 2024/1183 und VO (EU) 910/2014, sowie Server Signing Application Service Provider (SSASP) nach ETSI TS 119 431-1.

Teilaufgaben des VDA werden an Partner oder externe Anbieter ausgelagert.

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

Der VDA bietet die Ausstellung von qualifizierten und fortgeschrittenen Zertifikaten für elektronische Signaturen und Siegel an. Qualifizierte Zertifikate werden im Sinne der VO (EU) Nr. 2024/1183 und VO (EU) 910/2014 (eIDAS-Verordnung) ausgestellt und benötigen zur Erstellung eine QSCD gemäß den regulatorischen Vorgaben. Fortgeschrittene Zertifikate nach NCP+ erfordern ein sicheres kryptografisches Gerät (SSCD). Alle Zertifikate werden ausschließlich über die beim VDA betriebenen CAs ausgestellt.

Die für den Fernsignatur- und Fernsiegeldienst ausgestellten qualifizierten und fortgeschrittenen Zertifikate können zur Erstellung von elektronischen Fernsignaturen und Fernsiegeln verwendet werden. Siegel können ausschließlich von juristischen Personen, Signaturen ausschließlich von natürlichen Personen angewendet werden.

Der VDA 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 Zertifikate bis zu deren Archivierung, für den Vertrauensdienst der Ausstellung von qualifizierten Zertifikaten für qualifizierte elektronische Signaturen und Siegel im Sinne der VO (EU) Nr. 2024/1183, VO (EU) 910/2014, 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.

Für den Vertrauensdienst des Zeitstempels nach ETSI EN 319 421 und ETSI EN 319 422 gilt die „Timestamping Policy der SIGN8 GmbH“.

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

Maßgeblich ist allein die deutsche Fassung dieses Zertifizierungskonzepts.

Als alleinstehendes Dokument ist dieses Zertifizierungskonzept im Verhältnis zwischen dem VDA und dem Zertifikatsinhaber bzw. der Relying Party rechtsverbindlich. Für das Verhältnis zwischen dem VDA und dem Zertifikatsinhaber bzw. der Relying Party sind ebenso die vertraglichen oder bei Fehlen eines Vertragsverhältnisses, die gesetzlichen Bestimmungen sowie die wirksam einbezogenen Allgemeinen Geschäftsbedingungen (AGB) maßgeblich. Soweit nicht ausdrücklich anders vermerkt, beinhaltet dieses Zertifizierungskonzept keine Zusicherungen, Garantien oder Gewährleistungen. In Bezug auf das Verhältnis zwischen dem Conformity Assessment Body (CAB) und dem VDA ist dieses Dokument ebenso rechtsverbindlich.

1.1.2. Eigenschaften der PKI von SIGN8

Die qualifizierte PKI des VDA 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. Es werden nur die qualifizierten CAs (gekennzeichnet durch QES im Namen) als auch die Timestamping CAs auf die Trusted List aufgenommen.

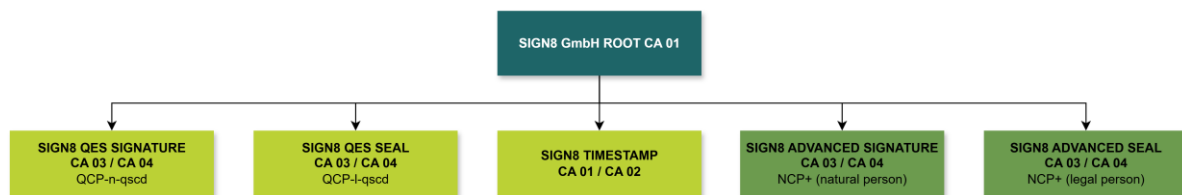


Abbildung 1: PKI-Hierarchie der PKI des VDA

Die ausgegebenen Zertifikate entsprechen den Anforderungen der eIDAS-Verordnung. 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 2. Generation der Zertifikate entspricht 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.

1.2. Name und Kennzeichnung des Dokuments

Dokumentenname: Certificate Practice Statement der SIGN8 GmbH

Kennzeichnung: 1.3.6.1.4.1.58197.1.4.0

Version: 1.6

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:

- URL: <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>
- URL: <http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC>
- URL: <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 qualifizierte Siegelzertifikate, welche auf juristische Personen ausgestellt werden.

1.3.4. Zertifikatsprüfer (Relying Party)

Relying Parties sind natürliche oder juristische Personen oder sonstige Dritte (z.B. Systeme), welche die Zertifikate der PKI der SIGN8 GmbH nutzen und Zugang zu den Zertifizierungsdienstleistungen der SIGN8 GmbH haben.

1.3.5. Andere Teilnehmer

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

Der VDA 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 VDA 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 oder fortgeschrittene Zertifikate in ihrem Namen auszustellen. Unterzeichner haben die Möglichkeit mithilfe des angebotenen Vertrauensdienstes, fortgeschrittene und qualifizierte Fernsignaturen oder -siegel zu erstellen. Alle Unterzeichner sind Zertifikatsinhaber und Endanwender.

1.4. Verwendung von Zertifikaten

Zertifikatsinhaber dürfen, die von dem VDA ausgegebenen qualifizierten und fortgeschrittenen 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 fortgeschrittenen Zertifikats zu einem bestimmten Zweck geeignet ist, obliegt dem Zertifikatsinhaber. Der VDA übernimmt keine Haftung für den Fall, dass ein Zertifikatsinhaber ein qualifiziertes oder fortgeschrittenes Zertifikat zu anderen als den 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 GmbH.

Es werden keine Attribute angeboten, welche über die Angaben in den Abschnitten

3. Identifizierung und Authentifizierung und 7. Profile von Zertifikaten, Widerrufslisten und OCSP hinausgehen.

1.4.1. Gültigkeitsmodell

Ab Inbetriebnahme der eIDAS-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 VDA selbst und zur eigenen Verwendung ausgestellt. Sie unterliegen den Anforderungen der jeweils 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 VDA-relevanten Konzepte werden durch den VDA verwaltet und vom Leiter der Vertrauensdienste genehmigt. Diese werden je nach Bedarf veröffentlicht und an Mitarbeiter des VDA oder Dritte kommuniziert.

Das Zertifizierungskonzept wird regelmäßig, mindestens jedoch alle zwölf Monate, gewartet und falls erforderlich aktualisiert von der Leitung der Vertrauensdienste. Eine Überprüfung des Zertifizierungskonzepts erfolgt insbesondere bei einer Änderung der für den VDA wesentlichen Gesetze sowie bei der Änderung betrieblicher Abläufe. Im Falle einer Änderung wird die geänderte Fassung unverzüglich auf der Internetseite des VDA veröffentlicht.

Eine Änderung des Zertifizierungskonzepts kann ausschließlich der VDA selbst vornehmen. Die Änderung wird durch die Vergabe einer neuen Versionsnummer kenntlich gemacht.

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

SIGN8 GmbH
Fürstenrieder Str. 5
80687 München
Tel.: +49 89 2153 7472 000
E-Mail: info@sign8.eu

1.6. Definitionen und Abkürzungen

Begriff	Beschreibung/Definition
AGB	Allgemeine Geschäftsbedingungen für den Zertifizierungsdienst
API	Application Programming Interface
Andere Teilnehmer	Siehe Abschnitt 1.3.5. <i>Andere Teilnehmer</i>
BDSG	Bundesdatenschutzgesetz
BMA	Brandschutzmeldeanlage
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
CAB	Conformity Assessment Body
CA/Certificate Authority	Zertifizierungsstelle
CPS	Certification Practice Statement
DSGVO	Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
eIDAS-Verordnung	Verordnung (EU) 910/2014 und Verordnung (EU) Nr. 2024/1183 des europäischen Parlamentes und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 hinsichtlich der Schaffung eines europäischen Rahmens für die digitale Identität
EMA	Einbruchmeldeanlage

Endanwender	Subject, die Identität des Endanwenders ist mit dem Zertifikat und dem zugehörigen Schlüsselpaar verknüpft, siehe auch Abschnitt 1.3.3. <i>Zertifikatsinhaber und Endanwender</i>
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	Inhaltsdaten sind alle Informationen über den Antragssteller, die in ein fortgeschrittenes oder qualifiziertes 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-I-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 i. S. d. Artikel 3 lit. 23 eIDAS-Verordnung

RA/Registration Authority	Siehe Registrierungsstelle, Abschnitt 1.3.2. <i>Registrierungsstellen (RA)</i>
Relying Party	Siehe Abschnitt 1.3.4. <i>Zertifikatsprüfer (Relying Party)</i>
Root-CA	Oberste Zertifizierungsinstanz einer PKI
SAD	Signatur-Aktivierungsdaten
SCP	SSASC Policy
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.
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
UUID	Universally unique identifier

VDA	Vertrauensdiensteanbieter
VDG	Vertrauensdienstegesetz
Vertrauende Dritte	Siehe Abschnitt 1.3.4. <i>Zertifikatsprüfer (Relying Party)</i>
Vertrauensdienst	Elektronischer Dienst entsprechend Artikel 3 Abs. 16 eIDAS-Verordnung
Vertrauensdiensteanbieter	Anbieter von Vertrauensdiensten entsprechend Artikel 3 Abs. 19 eIDAS-Verordnung
Zertifikat	qualifiziertes Zertifikat für elektronische Signaturen i. S. d. Artikel 3 Nr. 15 eIDAS-Verordnung
Zertifikatsinhaber	Siehe Abschnitt 1.3.3. <i>Zertifikatsinhaber und Endanwender</i>
Zertifizierungsstelle	Siehe Abschnitt 1.3.1. <i>Zertifizierungsstelle (CA)</i>

1.7. Übertragung von Aufgaben an Dritte

Die Gesamtverantwortung für die angebotenen Vertrauensdienste liegt beim VDA SIGN8. 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 VDA übertragenen Aufgaben ausschließlich zuverlässige, ausreichend geschulte und fachkundige Mitarbeiter einzusetzen.

Der VDA hat in den folgenden Bereichen Aufgaben auf Dritte übertragen:

- Betrieb des Rechenzentrums
- Identifizierung der Zertifikatsinhaber und Endanwender

1.8. Ansprechpartner

Anfragen an den VDA richten Sie bitte an:

SIGN8 GmbH

Fürstenrieder Str. 5

80687 München

Tel.: +49 (0)89 2153 7472 000

E-Mail: info@sign8.eu

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1. Verzeichnisse

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

Weiterhin können alle CA-Zertifikate und Beispiel-EE-Zertifikate des VDA auf der Webseite des VDA unter: <https://sign8.eu/trust> abgerufen werden.

2.2. Veröffentlichung von Informationen zu Zertifikaten

Der VDA veröffentlicht die folgenden Informationen zu den von ihr ausgegebenen qualifizierten und fortgeschrittenen Zertifikaten:

- Den online zur Verfügung stehenden OCSP-Dienst
- dieses Zertifizierungskonzept,
- CA-Zertifikate.

Alle Informationen, insbesondere dieses können auf der Website des VDA abgerufen werden bzw. im Falle der Statusinformationen können diese direkt via OCSP abgefragt werden. Der Statusinformationsdienst wird hochverfügbar betrieben. Er wird im Falle eines Ausfalls schnellstmöglich, spätestens nach 48 (achtundvierzig) Stunden, wieder zur Verfügung gestellt.

Alle Dokumente werden, nach vorheriger Absprache mit dem jeweiligen CAB, versioniert inklusive Zeitpunkt der Aktualisierung veröffentlicht. Anhand des Zeitpunktes der Ausstellung eines Zertifikats ist somit ermittelbar, welche Dokumentenversion für das jeweilige Zertifikat heranzuziehen ist.

2.3. Zeitpunkt und Häufigkeit von Veröffentlichungen

Dieses CPS wird veröffentlicht und bleibt mindestens so lange abrufbar, wie Zertifikate, die auf Basis dieses CPS ausgestellt wurden, gültig sind.

Im Falle einer Aktualisierung werden die neuen Fassungen unverzüglich kommuniziert an alle relevanten Parteien durch die Veröffentlichung auf der Website des VDA, wenn sie die Akzeptanz der Nutzer der Vertrauensdienste beeinflussen könnten. Alte Versionen werden durch den VDA archiviert und bleiben somit auch weiterhin verfügbar.

2.4. Zugang zu den Informationen

Die AGB, PDS, TP sowie das CPS und weitere Informationen, wie beispielsweise CA-Zertifikate sind unentgeltlich und in leicht verständlicher Sprache unter der folgenden Internetseite öffentlich zugänglich: <https://sign8.eu>. Anhand eines Zertifikatsprofils können die jeweils geltenden AGB, PDS und CPS identifiziert werden. Beschränkungen für den lesenden Zugriff bestehen nicht. Inhaltliche Änderungen werden ausschließlich durch den VDA vorgenommen. Der VDA stellt sicher, dass der Zugriff jederzeit möglich ist. Störungen des Zugriffs werden unverzüglich behoben, spätestens aber innerhalb von 24 Stunden.

3. Identifizierung und Authentifizierung

3.1. Namensregeln

3.1.1. Arten von Namen

Qualifizierte und fortgeschrittene 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/oder Familiennamen oder ein Pseudonym. Zertifikate für juristische Personen enthalten die offizielle Bezeichnung der Organisation. 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 und juristische Personen werden im Abschnitt 7.1. *Zertifikatsprofile* aufgeführt.

3.1.5. Eindeutigkeit von Namen

Die Eindeutigkeit des Zertifikats wird mittels der Seriennummer (serialNumber) erzielt. Der VDA 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 VDA ist nicht verpflichtet, solche Rechte zu überprüfen. Daraus resultierende Schadenersatzansprüche gehen zu Lasten des Endanwenders.

3.1.7. Password-Policy

Für Passwörter für den Zugang zu einem Kundenkonto bei SIGN8 gilt, dass Passwörter aus mindestens 8 Zeichen, mind. ein Großbuchstabe und ein Kleinbuchstabe, mindestens eine Zahl und mind. ein Sonderzeichen bestehen muss.

3.1.8. Test-Zertifikate

Zertifikate zu Testzwecken sind ausnahmsweise zulässig, wenn deren Ausstellung für die Vorbereitung oder die Prüfung des ordentlichen produktiven Einsatzes notwendig sind. Die Anzahl der Test-Zertifikate entspricht der Anzahl der vorhandenen Zertifikatstypen. Die Test-Zertifikate müssen sowohl im Anzeigenamen (commonName) wie auch in einer evtl. vorhandenen Organisationsbezeichnung eindeutig den Ausdruck „TEST“ enthalten. Pseudonyme sind für Test-Zertifikate nicht zugelassen.

3.2. Identifizierung der Zertifikatsinhaber

Der VDA hat Personen, die ein qualifiziertes oder fortgeschrittenes 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

Der Endanwender nutzt die Umgebung von SIGN8 und greift über eine Benutzerschnittstelle auf seinen privaten Schlüssel zu. Das durch die QSCD generierte Schlüsselpaar wird durch den VDA verwaltet. Der VDA stellt sicher, dass die Schlüsselpaare nur durch ein geeignetes QSCD und ausschließlich mithilfe eines geeigneten Multifaktor-Authentifizierungsverfahrens durch den Endanwender verwendet werden können.

Inhaber von SIGN8 Token erhalten eine QSCD in Form eines USB-Sticks oder einer Smartcard, auf dem sich der private Schlüssel befindet. Für die Aktivierung des privaten Schlüssels ist neben dem Besitz des Tokens die Eingabe einer PIN erforderlich.

Der Endanwender ist für das sichere Verwahren seiner Authentisierungs- und Anmeldedaten verantwortlich.

3.2.2. Identifizierung und Authentifizierung von Organisationen

Um die juristische Person, die im Distinguished Name (DN) des Zertifikats unter Organization (O) genannt wird, zu identifizieren, wird die jeweilige Handelsregisternummer zur Überprüfung benötigt.

Alle Personen, unabhängig von der Art der Organisation, die eine Organisation vertreten, müssen gemäß Artikel 24 Abs. 1 der VO (EU) Nr. 2024/1183 und VO (EU) 910/2014 identifiziert werden.

Für alle Rechtsformen werden folgende Daten erhoben:

1. Firma, Name oder Bezeichnung,
2. Rechtsform,
3. Handelsregisternummer oder Umsatzsteuer- Identifikationsnummer,

4. Anschrift des Sitzes oder der Hauptniederlassung oder der im Handelsregister angegebenen Geschäftsanschrift,
5. die Namen der Mitglieder des Vertretungsorgans oder die Namen der gesetzlichen Vertreter und, sofern ein Mitglied des Vertretungsorgans oder der gesetzliche Vertreter eine juristische Person ist, von dieser juristischen Person die Daten nach Ziffer 1. bis 4. und
6. E-Mail-Adresse zur direkten Kontaktaufnahme durch den VDA.

Darüber hinaus können zusätzlich weitere freiwillige Angaben erhoben werden wie bspw. Telefonnummer, E-Mail-Adresse oder Branche.

Für alle Rechtsformen wird in jedem Fall überprüft:

- die im Zertifikatsantrag angegebene Adresse der Organisation wird anhand des elektronischen Handelsregisters oder vergleichbarer Verzeichnisse überprüft, siehe Anlage über die Vorgehensweise der Überprüfung. Der Auftraggeber muss an dem angegebenen Standort eine Filiale, Geschäftsstelle oder Ähnliches betreiben;
- die Autorisierung des verantwortlichen Ansprechpartners der im Auftrag aufgeführten Organisation (juristische Person) und
- im Falle, dass ein Dritter im Namen der Organisation die Zertifikatsbeauftragung und/oder -verwaltung für diese durchführt, bedarf es einer entsprechenden, schriftlichen Vollmacht über die Übertragung der Rechte.

Für die Überprüfung der Existenz, der Adresse oder weiterer oben genannter Angaben der Organisation werden ausschließlich die Handelsregisterauszüge, vergleichbare Verzeichnisse oder amtliche Bestätigungen herangezogen. Online abgerufenen Register und Verzeichnisse werden dabei ausschließlich über HTTPS aufgerufen.

Mindestens ein juristischer Vertreter wird durch einen zertifizierten Identifizierungsdienstleister im Auftrag des VDA gemäß Abschnitt 3.2.3. *Identifizierung und Authentifizierung natürlicher Personen* identifiziert.

Existiert ein gültiges Zertifikat, kann die Authentifizierung jeder siegelberechtigten Person einer Organisation für die Transaktion durch eine, durch den VDA 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 Artikel 24 Abs. 1 der VO (EU) Nr. 2024/1183 und VO (EU) 910/2014 verifiziert werden. Dies umfasst ebenso den Vertretungsberechtigten des Endanwenders. Nach § 11 Abs. 4 VDG ist es möglich Identitätsdaten zu nutzen, die zu einem früheren Zeitpunkt erhoben wurden.

Der VDA nutzt für die Identifizierung des Unterzeichners Verfahren gemäß Art. 24 Abs. 1a lit. c) VO (EU) Nr. 2024/1183, sofern nicht bereits ein gültiges Zertifikat existiert. Die Identifizierung des Unterzeichners erfolgt durch vom VDA beauftragte externe Identifizierungsdienstleister oder SIGN8 Ident Agenturen oder durch SIGN8 Mitarbeiter bei Beantragung durch eine qualifizierte Signatur. Eine Liste der beauftragten Identifizierungsdienstleister können den TOM entnommen werden. Der Unterzeichner wird über einen gesicherten Kanal an den ausgewählten Identifizierungsdienstleister weitergeleitet.

Folgende Daten werden 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 VDA zugelassene, Authentifizierungsmethode.

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

Abweichend gilt für fortgeschrittene Zertifikate, dass die Identifizierung des Unterzeichners durch vom VDA beauftragte externe Identifizierungsdienstleister oder durch Angabe eines Mobiltelefonanschlusses, der im Zusammenhang mit den Zertifizierungsdiensten eingesetzt werden soll, erfolgt und folgende Daten erhoben werden:

- Vor- und Nachname und/oder
- Mobilfunknummer

3.2.4. Ungeprüfte Angaben zum Zertifikatsnehmer

Alle Informationen, welche in ein Zertifikat übernommen werden und im Rahmen der Authentifizierung nach den Abschnitten 3.2.2. *Identifizierung und Authentifizierung von Organisationen* und 3.2.3. *Identifizierung und Authentifizierung natürlicher Personen* erhoben werden, müssen verifiziert werden.

3.2.5. Überprüfung fremder CAs, RAs

Keine Vorgaben.

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 Zertifikate ausschließlich für juristische Personen (Endanwender) ausgestellt. Der Endanwender muss dem VDA gegenüber seinen Existenznachweis nach Abschnitt 3.2.2. *Identifizierung und Authentifizierung von Organisationen* erbringen, die Vertretungsberechtigung des Zertifikatsnehmers nachweisen, sowie den Identitätsnachweis ggf. mit Organisations-zugehörigkeit des Zertifikatnehmers nach den Abschnitten 3.2.2. *Identifizierung und Authentifizierung von Organisationen* und 3.2.3. *Identifizierung und Authentifizierung natürlicher Personen* erbringen. Nach der Prüfung der Antragsdokumente entscheidet der VDA, ob er den Antrag annimmt oder ablehnt.

3.2.7. Interoperabilität

Eine Verwendbarkeit der von dem VDA erzeugten Zertifikate außerhalb der von dem VDA betriebenen PKI ist nicht vorgesehen.

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

Eine Schlüsselerneuerung ist nicht vorgesehen. Nach Ablauf der Zertifikatsgültigkeit werden dem Endanwender neue Zertifikate ausgestellt.

3.4. Identifizierung und Authentifizierung bei Stellung eines Widerrufsverlangens

Zum Widerruf eines Zertifikates sind nur Widerrufsberechtigte nach Abschnitt 4.9.2. Widerrufsberechtigte berechtigt.

Der Widerruf eines Zertifikates ist über die Website des VDA möglich. Die Identifizierung und Authentifizierung erfolgt durch eine, durch den VDA zugelassene, Methode.

Der Zertifikatnehmer und Endanwender wird über den Widerruf per E-Mail informiert. Der Widerruf eines Zertifikats kann nicht rückgängig gemacht werden.

Das Sperrverfahren wird in Abschnitt 4.9. *Widerruf und Suspendierung von Zertifikaten* definiert.

4. Betriebsanforderungen

Gemäß Artikel 21 Absatz 3 eIDAS-Verordnung darf SIGN8 mit der Erbringung des qualifizierten Vertrauensdienstes beginnen, nachdem der qualifizierte Status in den in Artikel 22 Absatz 1 eIDAS-Verordnung genannten Vertrauenslisten ausgewiesen wurde.

Jeder Mitgliedstaat sorgt für die Aufstellung, Führung und Veröffentlichung von Vertrauenslisten, die Angaben zu den qualifizierten Vertrauensdiensteanbietern, für die er verantwortlich ist, und den von ihnen erbrachten qualifizierten Vertrauensdiensten, umfassen.

Die Mitgliedstaaten erstellen, führen und veröffentlichen auf gesicherte Weise elektronisch unterzeichnete oder besiegelte Vertrauenslisten gemäß Artikel 22 Absatz 1 eIDAS-Verordnung in einer für eine automatisierte Verarbeitung geeigneten Form.

Die Mitgliedstaaten übermitteln der Kommission unverzüglich Informationen über die für die Erstellung, Führung und Veröffentlichung der nationalen Vertrauenslisten verantwortlichen Stellen, den Ort der Veröffentlichung der Listen, die zur Unterzeichnung oder Besiegelung der Vertrauenslisten verwendeten Zertifikate und alle etwaigen Änderungen dieser Informationen.

Die Kommission macht diese Informationen auf sichere Weise und elektronisch unterzeichnet oder besiegelt in einer für eine automatisierte Verarbeitung geeigneten Form öffentlich zugänglich.

4.1. Zertifikatsantrag

Der VDA gibt Zertifikate für elektronische Signaturen und Fernsignaturen ausschließlich an natürliche Personen aus.

Zertifikate für elektronische Siegel und Fernsiegel werden ausschließlich an juristische Personen und deren autorisierte Vertreter ausgegeben.

Die Antragsstellung geschieht ausschließlich online. Die Zustimmung zu den Allgemeinen Geschäftsbedingungen ist Voraussetzung für den Abschluss des Vertrages. Die Allgemeinen Geschäftsbedingungen sind in deutscher Sprache verfasst und werden den Antragstellern in elektronischer Form zum Download zur Verfügung gestellt und ausdrücklich auf sie hingewiesen. Ein Abschluss ohne Zustimmung ist technisch nicht möglich.

Dem Zertifikatnehmer wird vor Abschluss des Registrierungsprozesses alle Dokumente wie CPS und PDS der Zugriff ermöglicht. Diese Dokumente sind öffentlich zugänglich. Alle Nachweise und Vertragsdokumente werden für die Dauer, die vertraglich vereinbart wurde, elektronisch oder papierbasiert hinterlegt.

Die Identifikation des Antragstellers erfolgt nach den Angaben des Abschnittes 3.2.3. *Identifizierung und Authentifizierung natürlicher Personen*. Der VDA behält es sich vor, Anträge auf Ausstellung eines Zertifikates abzulehnen.

Alle Schritte der Zertifikatsgenerierung und auch die vorbereitenden Schritte bei den verwendeten QSCDs werden geloggt.

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 VDA beauftragten externen Identifizierungsdienstleister sowie SIGN8 Ident Agenturen oder durch SIGN8 Mitarbeiter bei Beantragung durch eine qualifizierte Signatur durchgeführt. 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 VDA zugelassenen Methode.

Der VDA ist für die ordentliche Identifizierung nach Artikel 24 Abs. 1 eIDAS-Verordnung 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 gemäß Artikel 26 (a), (b) eIDAS-Verordnung und Siegel gemäß Artikel 36 (a), (b) eIDAS-Verordnung, eindeutig dem Zertifikatsinhaber und Unterzeichner zugeordnet werden können und der Unterzeichner eindeutig identifiziert werden kann.

4.2.2. Annahme oder Ablehnung des Antrags

Der VDA lehnt einen Antrag auf Erstellung eines Zertifikats ab, wenn die Antragsunterlagen nicht oder nicht vollständig vorliegen oder inkorrekt sind oder wenn Identifikationsunterlagen unvollständig, beschädigt bzw. inkorrekt sind. Anträge werden zudem dann abgelehnt, wenn die Antragsdaten nicht mit den Ausweisdokumenten übereinstimmen. Weitere Gründe für die Ablehnung eines Antrages können sein:

- Verdacht auf die Verletzung der Namensrechte Dritter;
- Nichteinhalten von Fristen für den Nachweis der Daten.

Der VDA behält sich das Recht vor, Anträge auch aus anderen Gründen abzulehnen.

Nachdem alle Daten gemäß den Abschnitten 3.2.2. *Identifizierung und Authentifizierung von Organisationen* und 3.2.3. *Identifizierung und Authentifizierung natürlicher Personen* erfasst wurden, wird das Zertifikat aktiviert und ausgestellt.

4.3. Ausstellung von Zertifikaten

4.3.1. Vorgehen der CA bei der Ausstellung des Zertifikats

Die Zertifikatserstellung erfolgt durch die im Trust Center des VDA befindlichen CAs. Dabei wird sichergestellt, dass bei der Zertifikatserstellung die korrekte Zeit verwendet wird, sowie die korrekte Verknüpfung des Schlüssels mit dem Zertifikat. Bei Verwendung des Fernsignatur- und Fernsiegeldienstes wird das Schlüsselpaar auf den vom VDA betriebenen QSCD generiert und der private Schlüssel verbleibt dort. Bei einem SIGN8 Token wird das Schlüsselpaar direkt auf dem Token generiert (QSCD in Form eines USB-Sticks oder Smartcard). Der private Schlüssel verbleibt auf dem Token.

Alle Zertifikate werden in einer vom VDA betriebenen Datenbank gespeichert. Diese Datenbank ist auch die Grundlage für den zur Verfügung gestellten OCSP Dienst.

4.3.2. Benachrichtigung des Zertifikatsinhabers über die Erstellung des Zertifikats

Eine Benachrichtigung des Zertifikatsinhabers über die Erstellung des Zertifikates erfolgt nicht.

4.4. Zertifikatsübergabe

4.4.1. Verhalten bei der Zertifikatsübergabe

Bei Verwendung von Fernsignatordiensten bzw. Fernsiegeldiensten werden die Zertifikate den Endanwendern nicht direkt übergeben. Der Endanwender kann nach eindeutiger Identifizierung und Authentifizierung, über die von SIGN8 angebotene Schnittstelle, auf sein Zertifikat zugreifen. Bei einer Signatur wird das Zertifikat des Endanwenders in die signierte Datei eingebettet.

Beim SIGN8 Token wird das Zertifikat durch ein Programm auf das Endgerät bzw. auf die USB-Stick oder Smartcard QSCD importiert.

4.4.2. Veröffentlichung des Zertifikats durch den VDA

Der VDA bietet einen intern wie extern erreichbaren Verzeichnisdienst für Statusinformationen über OCSP an. Eine gesonderte Veröffentlichung der ausgestellten Zertifikate der Endanwender erfolgt nicht.

4.4.3. Benachrichtigung Dritter über die Erstellung des Zertifikats

Dritte werden über die Erstellung der Zertifikate nicht benachrichtigt.

4.5. Verwendung des Schlüsselpaars und des Zertifikats

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

Die ausgestellten privaten Schlüssel und Zertifikate von Fernsignaturdiensten bzw. Fernsiegeldiensten sind ausschließlich für die Verwendung bei SIGN8 vorgesehen. Es gelten die Regelungen aus Abschnitt 1.4. *Verwendung von Zertifikaten* sowie die AGB und etwaige einzelvertragliche Vereinbarungen.

Bei SIGN8 Token ist eine Schlüsselverwendung nur für die in den Zertifikaterweiterungen dokumentierten Bereichen zulässig.

4.5.2. Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsinhaber

Die Zertifikate können von allen Zertifikatsinhabern verwendet werden. Die Zertifikatsinhaber und Vertrauende Dritte dürfen jedoch nur dann auf den öffentlichen Schlüssel und das Zertifikat vertrauen, wenn folgende Voraussetzungen vorliegen:

- das Zertifikat wird gemäß der zulässigen Nutzungsarten verwendet und eventuelle Einschränkungen im Zertifikat wurden beachtet;
- die Zertifikatskette kann erfolgreich bis zu einem vertrauenswürdigen Intermediate-Zertifikat verifiziert werden;
- die Gültigkeit des Zertifikats wurde über den Statusabfragedienst (OCSP) bestätigt;
- alle weiteren Vereinbarungen und sonstigen Vorsichtsmaßnahmen wurden eingehalten.

4.6. Zertifikatserneuerung

Eine Zertifikatserneuerung wird nicht angeboten.

4.7. Zertifikatserneuerung mit Schlüsselerneuerung

Eine Zertifikatserneuerung durch Schlüsselerneuerung wird nicht angeboten. Nach Ablauf eines Zertifikats kann der Endanwender ein neues Zertifikat beantragen.

4.8. Zertifikatsänderung

Eine nachträgliche Änderung des Zertifikats durch den VDA wird nicht angeboten.

4.9. Widerruf und Suspendierung von Zertifikaten

Bei einem Widerruf von Zertifikaten werden Schlüssel gemäß Kapitel 6.2.10 zerstört. Dadurch verlieren sie ab dem Zeitpunkt des Widerrufs ihre Gültigkeit.

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;
- das betroffene Zertifikat nicht mehr benötigt wird;
- die Gefahr einer missbräuchlichen Verwendung des Zertifikats besteht;
- Inhaltsdaten des Zertifikats nicht mehr korrekt sind.

Gemäß § 14 Abs. 3 VDG ist auch die Bundesnetzagentur in der Lage die ausgestellten Zertifikate zu widerrufen.

In folgenden Fällen erfolgt ein Widerruf des Zertifikats durch den VDA bei Vorliegen eines in VDG § 14 genannten Sperrgrundes sowie den folgenden Gründen:

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

Der VDA 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 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 VDA 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 VDA und widerrufsberechtigte Dritte berechtigt. Darüber hinaus kann die zuständige Behörde einen Zertifikatswiderruf der VDA-Zertifikate und der Endnutzer-Zertifikate veranlassen entsprechend § 14 Abs. 3 VDG.

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 GmbH 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 Widerrufsverlangens

Eintreffende Widerrufsansträge 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.

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 VDA 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 Zertifikatsstatus kann mindestens zehn Jahre nach Ablauf der Gültigkeit über den Statusabfragedienst abgerufen werden. 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 VDA wird Störungen des Statusabfragedienstes 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 VDA 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 VDA ausgestellten Endanwender-Zertifikate sind höchstens fünf Jahre gültig.

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

Der VDA benachrichtigt Endanwender und Dritte, einschließlich Vertrauender Dritter und der zuständigen Aufsichtsbehörde und ggf. den fortführenden VDA, rechtzeitig, mindestens aber zwei Monate vorher, über die Einstellung der Vertrauensdienste.

Der VDA 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 VDA, 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 Fernsignatur- und Fernsiegeldienst treuhänderisch vom VDA verwaltet. Der private Schlüssel wird sicher verwaltet. Es ist über den VDA 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

Alle sensiblen Daten und die für den Betrieb der für des VDA relevanten Systeme sind in physikalisch geschützten Sicherheitsbereichen innerhalb eines Rechenzentrums (Trust Center) untergebracht. Durch Zutrittskontrollmechanismen wird sichergestellt, dass keine unberechtigten Personen Zugang zu den Sicherheitsbereichen haben. Alle Zutritte, auch unerlaubte Zutrittsversuche, werden protokolliert. Versuche zur Überwindung der Sicherheitsmechanismen wie Einbruch, Diebstahl und Vandalismus lösen einen Alarm aus. Innerhalb des Sicherheitsbereichs gibt es einen zusätzlichen physikalischen Schutz der IT-Systeme und Schlüssel des VDA. Diese Maßnahme und die zusätzliche Videoüberwachung bieten einen zusätzlichen Schutz vor Manipulation und Diebstahl. Der Sicherheitsbereich verfügt über zertifizierte Feuer- und Blitzschutzvorrichtungen. Er ist nach ISO / IEC 27001 zertifiziert und stimmt mit den Vorgaben der VEB security class 4 überein. Das Sicherheitskonzept und das zugrundeliegende Notfallkonzept werden regelmäßig überprüft, jedoch mindestens alle zwölf Monate.

Der VDA ergreift geeignete technische und organisatorische Maßnahmen zur Beherrschung der Sicherheitsrisiken im Zusammenhang mit den von ihm erbrachten Vertrauensdiensten. Diese Maßnahmen müssen unter Berücksichtigung des jeweils neuesten Standes der Technik gewährleisten, dass das Sicherheitsniveau der Höhe des Risikos angemessen ist. Insbesondere sind Maßnahmen zu ergreifen, um Auswirkungen von Sicherheitsverletzungen zu vermeiden bzw. so gering wie möglich zu halten und die Beteiligten über die nachteiligen Folgen solcher Vorfälle zu informieren.

Der VDA meldet der Aufsichtsstelle und wo zutreffend anderen einschlägigen Stellen wie etwa der für Informationssicherheit zuständigen nationalen Stelle oder der Datenschutzbehörde unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme von dem betreffenden Vorfall, jede Sicherheitsverletzung oder jeden Integritätsverlust, die bzw. der sich erheblich auf den erbrachten Vertrauensdienst oder die darin vorhandenen personenbezogenen Daten auswirkt.

Wenn sich die Sicherheitsverletzung oder der Integritätsverlust voraussichtlich nachteilig auf eine natürliche oder juristische Person auswirken, für die der Vertrauensdienst erbracht wurde, so unterrichtet der Vertrauensdiensteanbieter auch diese natürliche oder juristische Person unverzüglich über die Sicherheitsverletzung oder den Integritätsverlust.

Gegebenenfalls unterrichtet die notifizierte Aufsichtsstelle die Aufsichtsstellen anderer betroffener Mitgliedstaaten und die ENISA, insbesondere, wenn von der Sicherheitsverletzung oder dem Integritätsverlust zwei oder mehr Mitgliedstaaten betroffen sind.

Die notifizierte Aufsichtsstelle unterrichtet ferner die Öffentlichkeit oder verpflichtet den Vertrauensdiensteanbieter hierzu, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung oder des Integritätsverlustes im öffentlichen Interesse liegt.

Die Aufsichtsstelle übermittelt der ENISA einmal jährlich eine Übersicht über die von den Vertrauensdiensteanbietern gemeldeten Sicherheitsverletzungen und Integritätsverlusten.

5.2. Verfahrensvorschriften

5.2.1. Rollenkonzept

Teil der Dokumentation ist ein Rollenkonzept, in dem Mitarbeiter einer oder mehreren Rollen durch das Management des VDA zugeordnet werden und entsprechende Berechtigungen durch einen gesteuerten Prozess erhalten. Die Berechtigungen der einzelnen Rollen, physikalisch und logisch, beschränken sich auf diejenigen, die sie zur Erfüllung ihrer Aufgaben benötigen. Es wird sichergestellt, dass ein Mitarbeiter nie sich ausschließende Rollen innehaben kann.

Rollen mit Sicherheitsverantwortung für den Betrieb des VDA dürfen nur von fachkundigen und zuverlässigen Mitarbeitern übernommen werden. Diese Mitarbeiter müssen frei von Interessenskonflikten gestellt werden, damit die ausgeübten Rollen unbefangen und vorurteilsfrei ausgeübt werden können. Der Entzug einer Rolle wird dokumentiert.

5.2.2. Mehr-Augen-Prinzip

Besonders sicherheitskritische Vorgänge müssen mindestens im Mehr-Augen-Prinzip durchgeführt werden. Dies wird durch technische und organisatorische Maßnahmen wie beispielsweise Zutrittsberechtigungen und Abfrage von Wissen durchgesetzt.

Sicherheitskritische Systeme zur Zertifikatsausstellung sind zusätzlich durch eine Multifaktor-Authentisierung geschützt. Über Event-Logs kann die durchführende Person nachträglich einer Aktion zugeordnet werden.

5.2.3. Sonstige Dienstanweisung

Das Rollenkonzept sieht diverse Rollenausschlüsse vor, um Interessenskonflikte zu verhindern. Des Weiteren sieht das Rollenkonzept vor, das Mehr-Augen-Prinzip zu erzwingen und schädliches Handeln vorzubeugen.

5.2.4. Standards und Kontrollen für kryptographische Module

Die privaten Schlüssel der CAs werden auf einer QSCD generiert und abgelegt.

Zum Schutz der kryptographischen Geräte, während Betrieb, Transport und Lagerung werden die Hersteller-spezifischen Mechanismen verwendet, die während der FIPS- und CC-Zertifizierungen geprüft wurden.

5.3. Personalkonzept

Das Personalkonzept des VDA ist darauf ausgerichtet, sicherzustellen, dass das gesamte Personal, einschließlich der Mitarbeiter, der Führungskräfte und der direkten externen Dienstleister, die notwendigen Sicherheitsanforderungen und -verpflichtungen im Hinblick auf die Vertrauensdienste und die Informationssicherheit versteht und befolgt.

5.3.1. Qualifikation, Erfahrung und Zuverlässigkeit des Personals

Der VDA gewährleistet, dass alle Personen, die im Bereich der Vertrauensdienste oder in sicherheitskritischen Rollen tätig sind, die für ihre Tätigkeit notwendige Expertise, Erfahrung und Qualifikation besitzen.

Die Kompetenz wird durch Ausbildungs- und Schulungsnachweise, relevante Zertifizierungen oder entsprechende Arbeitserfahrung dokumentiert und überprüft.

Das Führungspersonal verfügt über Erfahrung oder Qualifikation in Bezug auf die erbrachten Vertrauensdienste und ist mit den Sicherheitsverfahren von Personal mit Sicherheitsverantwortung vertraut. Außerdem verfügt das Führungspersonal über Erfahrung in der Informationssicherheit und Risikobewertung.

Die Identität, Zuverlässigkeit und Fachkunde des Personals werden vor der Aufnahme der Tätigkeit überprüft. Die Identitätsprüfung erfolgt durch die Vorlage eines gültigen, behördlich ausgestellten Ausweisdokuments. Die Zuverlässigkeitsprüfung umfasst die Überprüfung von Lebenslauf, Arbeitszeugnissen und Referenzen, um die gemachten Angaben zur Historie zu validieren.

Eine erweiterte Zuverlässigkeitsprüfung wird verpflichtend für Kandidaten durchgeführt, die Rollen mit privilegiertem Zugriff auf kritische Systeme oder sicherheitskritischen Funktionen innehaben sollen. Die erweiterte Prüfung umfasst, soweit gesetzlich und national zulässig und im Einklang mit den Datenschutzbestimmungen, die Überprüfung der strafrechtlichen Vorgeschichte oder eine gleichwertige Vertrauenswürdigkeitsprüfung.

Erst wenn alle notwendigen Kontrollen durchgeführt wurden, erhält der Mitarbeiter die Zutritts- und Zugriffsberechtigungen gemäß dem Rollenkonzept. Das Personal verpflichtet sich, die Sicherheitsrichtlinien und den Verhaltenskodex des VDA einzuhalten.

Alle Arbeitsverträge sowie Verträge mit kritischen, für die Erbringung unserer Vertrauensdienste wesentlichen externen Dienstleistern (z.B. Identitätsanbieter) enthalten explizite Sicherheitsverpflichtungen und umfassende Vertraulichkeitsvereinbarungen (NDAs). Diese Verpflichtungen gelten auch über das Ende des jeweiligen Vertragsverhältnisses hinaus.

5.3.2. Sicherheitsüberprüfung

Der VDA wendet das Prinzip der Pflichtentrennung an. Kritische Aufgaben (z.B. Systemkonfiguration und Systemaudit) sind auf mehrere Rollen verteilt, sodass kein einzelner

Mitarbeiter durch Missbrauch seiner Berechtigungen einen schwerwiegenden Sicherheitsverstoß ohne Beteiligung Dritter verursachen kann.

Die Trennung der Pflichten wird in den Rollenbeschreibungen festgehalten und regelmäßig überprüft. Die Mitarbeiter sind verpflichtet, jeden potenziellen oder tatsächlichen Interessenkonflikt unverzüglich zu melden.

Die Mitarbeiter dürfen sich nicht an externen Aktivitäten (z.B. Nebenbeschäftigungen) beteiligen, die einen Interessenkonflikt mit ihren Aufgaben im VDA darstellen oder die Sicherheit, Vertraulichkeit oder Integrität der Vertrauensdienste gefährden könnten.

5.3.3. Schulungen und Weiterbildungen

Alle Mitarbeiter werden bei Bedarf geschult. Nachschulungen werden dann durchgeführt, wenn Änderungen an den Prozessen, der Technik sowie den Rahmenbedingungen für den Betrieb des Vertrauensdienstes erfolgen oder wenn diese zur Vermittlung oder Aufrechterhaltung der notwendigen Fachkunde eines Mitarbeiters erforderlich sind. Sicherheitsrelevante Nachschulungen über neue Gefahren und Sicherheitsmethoden sind alle zwölf Monate verpflichtend für alle Mitarbeiter. Wie ein Sicherheitsvorfall erkannt wird und wie darauf zu reagieren ist, sind Teile dieser Schulung.

Schulungen werden zu allen für den Betrieb des VDA relevanten Themen durchgeführt. Zu Themen mit Sicherheitsrelevanz, wie Passwörter und Datenschutz, werden bevorzugt Schulungen durchgeführt. Alle Schulungen stehen den Mitarbeitern in einem internen Onboarding-Portal zur Verfügung und können dort jederzeit aufgerufen werden. Ziel der Schulungen ist es die Fachkompetenz der Mitarbeiter zu fördern und so die Sicherheit der durch den VDA betriebenen Dienstleistungen weiter zu gewährleisten.

Schulungen werden durch bereits fachkundiges Personal geplant, vorbereitet und durchgeführt. Es werden Materialien erstellt, welche die Schulungen unterstützen und das Thema der Schulung veranschaulichen. Schulungen, die sicherheitsrelevante Themen, beispielsweise die Erstellung sicherer Passwörter behandeln, sind für alle Mitarbeiter des VDA verpflichtend.

Es werden Mechanismen (z.B. regelmäßige Phishing-Simulationen, interne Audits) eingesetzt, um die Einhaltung der Cyber-Hygiene-Praktiken zu überwachen und zu gewährleisten.

Neue Mitarbeiter müssen vor der Aufnahme ihrer Tätigkeit alle verpflichtenden Schulungen absolviert haben. Die Teilnahme, der Abschluss und die Leistungsnachweise aller Schulungen werden lückenlos dokumentiert.

5.3.4. Häufigkeit von Job-Rotation

Bei Beendigung des Arbeitsverhältnisses oder bei einem Wechsel der Funktion innerhalb des VDA wird ein standardisiertes Austritts- bzw. Rollenwechselverfahren angewandt, um die Informationssicherheit zu gewährleisten.

Die Zugriffsrechte (logisch auf IT-Systeme und physisch auf gesicherte Bereiche) werden unverzüglich aufgehoben oder geändert, sobald die Beendigung oder der Rollenwechsel wirksam wird.

Sicherheitskritische Zugänge werden dabei priorisiert und bei Ausscheiden sofort deaktiviert.

Alle vom VDA bereitgestellten Assets (z.B. Laptops, Smartphones, Tokens, Schlüssel, Ausweise) werden inventarisiert und vom Mitarbeiter oder externen Dienstleister zurückgefordert.

Der Mitarbeiter wird abschließend über die weiterhin bestehenden Sicherheits- und rechtlichen Verpflichtungen (insbesondere zur Vertraulichkeit von Betriebsgeheimnissen und Kundendaten) informiert.

Diese fortlaufenden Verpflichtungen werden durch eine schriftliche Erklärung oder eine entsprechende Klausel im Austrittsprotokoll bestätigt.

5.3.5. Anforderungen an externes Personal

Für dauerhaft eingesetztes externes Personal gelten die gleichen Regelungen wie für das interne Personal (einschließlich Schulung, Zuverlässigkeitsprüfung und vertraglicher Verpflichtungen).

Externes Personal, welches temporär in sicherheitsrelevanten Bereichen tätig ist (z.B. Wartungspersonal), wird stets von berechtigten Mitarbeitern des VDA begleitet und beaufsichtigt.

Temporäres externes Personal erhält nur den minimal notwendigen Zugriff für die Dauer seiner Aufgabe, welcher danach unverzüglich entzogen wird.

5.3.6. Sanktionen bei unerlaubten Handlungen

Ein formelles Disziplinarverfahren bei Verstößen gegen die Sicherheitsrichtlinien oder Prozesse des VDA ist etabliert, allen Mitarbeitern kommuniziert und wird aufrechterhalten.

Verstöße werden vom Personalverantwortlichen, in Abstimmung mit der Sicherheitsleitung, analysiert und bewertet. Aufgrund der Bewertung werden angemessene Maßnahmen (von Ermahnung bis zur Kündigung) getroffen. Die Maßnahmen berücksichtigen dabei stets die relevanten rechtlichen, behördlichen, vertraglichen und geschäftlichen Anforderungen.

Kann das Vertrauensverhältnis nicht wiederhergestellt werden, werden die betroffenen Mitarbeiter von sicherheitsrelevanten Tätigkeiten ausgeschlossen.

5.3.7. Dokumentation

Der VDA stellt dem Personal alle erforderlichen Dokumente (Rollenbeschreibungen, Verfahrensanweisungen) zur Verfügung. Alle kritischen Prozesse werden revisionssicher dokumentiert:

5.4. Protokollierung von Überwachungsmaßnahmen

5.4.1. Überwachung des Zutritts

Das Trust Center, in dem sich die relevanten Ressourcen für den Betrieb des VDA befinden, wird durch umfangreiche Überwachungsmaßnahmen geschützt. Alle Zutritte zu den sicherheitsrelevanten Bereichen des VDA sind nur durch autorisiertes Personal möglich und werden protokolliert sowie eine angemessene Zeit lang gespeichert. Der Zutritt durch Gäste des VDAs oder Fremden ist nur in Begleitung von zugriffsberechtigten Mitarbeitern möglich und wird ebenfalls protokolliert.

5.4.2. Überwachung von organisatorischen Maßnahmen

Die organisatorischen Maßnahmen, die zum sicheren Betrieb des Vertrauensdienstes notwendig sind, werden regelmäßig durch den Sicherheitsbeauftragten überprüft. Alle Änderungen dieser Maßnahmen werden im Sicherheitskonzept, oder den TOM dokumentiert.

5.4.3. Art der aufgezeichneten Ereignisse

Generell enthalten alle Protokolleinträge mindestens das Datum und die Uhrzeit des Eintrags, einen Verweis auf das System, welches den Eintrag generiert hat, sowie eine Beschreibung des Ereignisses.

5.4.3.1. CA-Schlüsselpaare und CA-Systeme

Für das Lifecycle-Management für CA-Schlüsselpaare bzw. von CA-Systemen werden mindestens die folgenden Ereignisse protokolliert:

- Erzeugung, Vernichtung, Speicherung und Sicherung, sowie Archivierung des Schlüsselpaares oder Teile des Schlüsselpaares
- Ereignisse im Lebenszyklus-Management von kryptografischen Geräten (z.B. QSCD), sowie der eingesetzten CA-Software

5.4.3.2. EE- und CA-Zertifikate

Für das Lifecycle-Management von EE- als auch CA-Zertifikaten und deren Validierung protokolliert der VDA mindestens die folgenden Ereignisse:

- Antrag auf Widerruf von Zertifikaten und dessen Ergebnis
- Alle Tätigkeiten im Zusammenhang mit der Verifikation von Informationen
- Annahme oder Ablehnung von Zertifikatsaufträgen
- Ausstellung eines Zertifikates
- Erzeugung von Sperrlisten (CRL) und OCSP-Einträgen

5.4.3.3. Sonstige sicherheitsrelevante Ereignisse

Zusätzlich werden vom VDA für den Betrieb der Infrastruktur alle sicherheitsrelevanten Ereignisse protokolliert. Das beinhaltet mindestens die folgenden Ereignisse:

- Erfolgreiche und erfolglose Zugriffsversuche auf Systeme der PKI
- Durchgeführte Aktionen an und durch PKI- und sonstigen sicherheitsrelevanter Systeme
- Systemabstürze, Hardware-Ausfälle und andere Anomalien
- Firewall- und Router-Aktivitäten
- Zutritt und Verlassen von Einrichtungen des Trust Centers (durch das externe Personal)
- Ergebnisse von Netzwerkprüfungen (Schwachstellenüberprüfungen)
- Start und Beendigung des Logging-Prozesses

5.5. Archivierung von Unterlagen

5.5.1. Arten von Unterlagen

Archiviert werden alle gesetzlich geforderten Unterlagen zur vollständigen Dokumentation des Zertifikatslebenszyklus für qualifizierte Zertifikate. Archiviert werden die vollständigen Antragsunterlagen (auch Folgeanträge), CPS, Zertifikate, Widerrufsinformationen, elektronische Dateien, Notfallkonzepte, Schulungsunterlagen und Protokolle zum Zertifikatslebenszyklus. Dabei werden die Vorgänge zeitlich erfasst. Wenn anwendbar, umfasst dies auch die entsprechenden Systemprotokolle, die im Rahmen der genannten Ereignisse entstehen.

Alle gesetzlich geforderten Unterlagen zur vollständigen Dokumentation des Zertifikatslebenszyklus werden zur Verfügung gestellt, wenn diese als Nachweis des ordnungsgemäßen Betriebs der Vertrauensdienste, während eines Gerichtsverfahrens benötigt werden.

5.5.2. Aufbewahrungszeiten

Dokumente zur Antragstellung und Prüfung, Daten zum Zertifikatslebenszyklus, Konformitätsbewertungsdokumente sowie die Zertifikate selbst, werden für die gesamte Betriebszeit des VDA aufbewahrt. Wird der Betrieb eingestellt, werden alle Dokumente und Daten an die zuständige Aufsichtsbehörde übergeben.

Alle einschlägigen Informationen, über die von dem VDA ausgegebenen und empfangenen Daten werden so aufgezeichnet und aufbewahrt, dass sie über einen angemessenen Zeitraum, auch mindestens elf Jahre über den Zeitpunkt der Einstellung der Tätigkeit des qualifizierten Vertrauensdiensteanbieters hinaus, verfügbar sind, um insbesondere bei Gerichtsverfahren entsprechende Beweise liefern zu können und die Kontinuität des Dienstes sicherzustellen.

5.5.3. Archivsicherheit

Die Aufzeichnungen über den Betrieb der Dienste werden vollständig und vertraulich archiviert in Übereinstimmung mit offengelegten Geschäftspraktiken.

Die Archivierung erfolgt in Übereinstimmung mit ETSI EN 319 401 Abschnitt 7.10. Durch geeignete technische und organisatorische Maßnahmen wird sichergestellt, dass archivierte Daten vor unbefugtem Zugriff, Kopieren, Veränderung und Löschung geschützt sind. Die Maßnahmen sind im Datensicherungskonzept des VDA dokumentiert.

Weitere Beweismittel wie beispielsweise Protokolldateien werden auf einer Datenbank im gesicherten Rechenzentrum (Trust Center) des VDA gesichert. Eine genauere Beschreibung der Sicherheitsvorkehrungen befinden sich im Datensicherungskonzept der SIGN8 GmbH.

5.5.4. Datensicherung des Archivs

Die Sicherung der Daten erfolgt nach dem Stand der Technik. Es werden redundante Datenbanksysteme implementiert und Backups werden durchgeführt. Um die Authentizität und Integrität von Daten, wie beispielsweise Log-Daten, aus der sicheren Umgebung des VDA zu gewährleisten werden sie, bevor sie die sichere Umgebung in elektronischer Form verlassen, qualifiziert gesiegelt. Dadurch wird jede Veränderung erkannt und die Daten lassen sich eindeutig dem VDA zurechnen.

5.6. Umstellung des Schlüssels (key changeover)

Ein Schlüsselwechsel der CA-Schlüssel ist gleichgestellt mit der neuen Generierung einer neuen CA-Instanz. Dies geschieht jeweils in einem angemessenen Abstand vor Ablauf des aktuellen CA-Zertifikates. Sobald das neue CA-Zertifikat erstellt und entsprechend verteilt und veröffentlicht wurde, wird ausschließlich das neue CA-Zertifikat verwendet. Das alte CA-Zertifikat wird nicht mehr zur Ausstellung neuer EE-Zertifikate verwendet.

5.7. Notfallkonzept

5.7.1. Behandlung von Vorfällen

Die Behandlung von sicherheitsrelevanten Vorfällen und Kompromittierungen ist im Notfallhandbuch dokumentiert. Verantwortlich für die Umsetzung sind die leitenden Rollen.

Nachdem dem VDA eine kritische Schwachstelle oder eine Kompromittierung bekannt geworden ist, muss dieser unverzüglich handeln und entsprechende Maßnahmen ergreifen. Je

nach Art der Kompromittierung werden in Absprache mit der Aufsichtsbehörde die Auswirkungen analysiert und ggf. weitere Schritte zur Behebung veranlasst.

SIGN8 kommt seiner Meldepflicht nach Artikel 19 Absatz 2 eIDAS-Verordnung nach, indem SIGN8 der Aufsichtsstelle und wo zutreffend anderen einschlägigen Stellen wie etwa der für Informationssicherheit zuständigen nationalen Stelle oder der Datenschutzbehörde unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme von dem betreffenden Vorfall, jede Sicherheitsverletzung oder jeden Integritätsverlust, die bzw. der sich erheblich auf den erbrachten Vertrauensdienst oder die darin vorhandenen personenbezogenen Daten auswirkt.

Wenn sich die Sicherheitsverletzung oder der Integritätsverlust voraussichtlich nachteilig auf eine natürliche oder juristische Person auswirken, für die der Vertrauensdienst erbracht wurde, so unterrichtet der Vertrauensdiensteanbieter auch diese natürliche oder juristische Person unverzüglich über die Sicherheitsverletzung oder den Integritätsverlust. Gegebenenfalls unterrichtet die notifizierte Aufsichtsstelle die Aufsichtsstellen anderer betroffener Mitgliedstaaten und die ENISA, insbesondere, wenn von der Sicherheitsverletzung oder dem Integritätsverlust zwei oder mehr Mitgliedstaaten betroffen sind.

Die notifizierte Aufsichtsstelle unterrichtet ferner die Öffentlichkeit oder verpflichtet den Vertrauensdiensteanbieter hierzu, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung oder des Integritätsverlustes im öffentlichen Interesse liegt.

5.7.2. Wiederherstellung von IT-Systemen

Die IT-Systeme des VDA werden täglich gesichert und gespeichert. Die Wiederherstellung der Systeme ist Bestandteil des Notfallhandbuchs und wird von den Personen mit den entsprechenden Rollen laut Rollenkonzept ausgeführt.

5.7.3. Wiederherstellung nach Kompromittierung von privaten CA-Schlüsseln

Im Fall einer Kompromittierung oder der Bekanntgabe von Unsicherheiten von Algorithmen oder assoziierten Parametern werden betroffene Schlüssel sofort gewechselt. Dazu veranlasst der VDA folgendes:

- betroffene CA-Zertifikate sowie deren ausgestellte und bisher nicht ausgelaufene Zertifikate werden widerrufen,
- involvierte Zertifikatsnehmer und betroffene Dritte werden über den Vorfall und dessen Auswirkungen innerhalb von 24 Stunden informiert,
- die zuständige Aufsichtsstelle wird innerhalb von 24 Stunden informiert und der Vorfall wird auf den Webseiten des VDA veröffentlicht mit dem Hinweis, dass Zertifikate, die von dieser CA ausgestellt wurden, ihre Gültigkeit verlieren und der Sperrstatus verifiziert werden kann.

Aus der Analyse der Gründe für die Kompromittierung werden, wenn möglich, Maßnahmen ergriffen, um zukünftige Kompromittierungen zu vermeiden. Unter Berücksichtigung der Gründe für die Kompromittierung werden neue CA-Signaturschlüssel generiert und neue CA-Zertifikate ausgestellt.

5.7.4. Weiterführung des Betriebs nach Kompromittierung oder Katastrophenfall

Die verantwortlichen Personen laut Rollenkonzept entscheiden je nach Art der Katastrophe darüber, wie der Betrieb wieder aufgenommen werden soll. Die Betriebsaufnahme kann entweder durch Neuinstallation oder Wiederherstellung nach dokumentiertem Verfahren oder einer Kombination aus beiden Verfahren erreicht werden. Bei Bedarf auch an einem alternativen Standort. Zuvor wird jedoch sichergestellt, dass geeignete Maßnahmen ergriffen werden, um die Ursachen des Ausfalls oder der Kompromittierung zukünftig auszuschließen. Darunter wird auch das Notfallhandbuch überprüft und ggf. angepasst.

5.7.5. Regelmäßige Kontrolle

Das Notfallhandbuch wird regelmäßig alle zwölf Monate getestet, überprüft und ggf. angepasst.

5.8. Beendigung des Zertifizierungsbetriebs

Der VDA verfügt über einen fortlaufend aktualisierten Beendigungsplan, in dem Einzelheiten für den Fall der Einstellung der Tätigkeit niedergelegt sind. Ziel ist es, die Dienstleistungskontinuität und eine geordnete Abwicklung sicherzustellen.

Im Fall einer geplanten Betriebseinstellung informiert der VDA alle Endanwender, Zertifikatsnehmer und Dritte mindestens zwei Monate vorab.

Bei Beendigung der Dienste von CAs informiert der VDA alle Zertifikatsnehmer und beendet alle Zugriffsmöglichkeiten von Unterauftragnehmern des VDA in Bezug auf die betroffenen CAs. Alle noch gültigen und von den betroffenen CAs ausgestellten Zertifikate werden widerrufen. Betroffene private CA-Schlüssel werden zerstört.

Mit Beendigung des Betriebes wird alle Funktionalität der CAs eingestellt, so dass eine Zertifizierung nicht mehr möglich ist.

5.8.1. Beendigung des Zertifizierungsbetriebs eines kreuz-zertifizierten VDAs

Bei Beendigung der Dienste von CAs eines kreuz-zertifizierten VDA, werden alle zusammenhängenden Zertifikate widerrufen.

6. Technische Sicherheitsmaßnahmen

6.1. Erzeugung und Installation von Schlüsselpaaren

6.1.1. Erzeugung von Schlüsselpaaren

Die Generierung aller Schlüsselpaare im Verantwortungsbereich des VDA geschieht in sicheren, nach FIPS 140-2 Level 3 oder FIPS 140-3 Level 3 und Common Criteria EAL4 konformen und zertifizierten QSCDs. Alle QSCDs die die CA-Schlüssel verwalten befinden sich im Hochsicherheitsbereich des VDA. Die Key-Ceremony erfolgt nach festgelegtem Verfahren. Schlüsselpaare für EE-Zertifikate werden bei SIGN8 Token auf den USB-Stick QSCDs oder Smartcard QSCDs erzeugt. Bei EE- Zertifikaten des qualifizierten Fernsignatur- und Fernsiegeldienstes betreibt der VDA alle für die Erzeugung von Schlüsselpaaren involvierten QSCDs. EE-Signierschlüssel werden nicht im Voraus generiert.

Die CA-Schlüssel werden unter Einhaltung des Rollenkonzepts im Mehr-Augen-Prinzip erzeugt. Das Signieren von CA-Zertifikaten durch die Root CA erfordert einen direkten Befehl durch die autorisierten Mitarbeiter entsprechend dem Rollenkonzept. Weiterhin wird die Erstellung von CA-Schlüsseln dokumentiert.

Schlüsselbackups werden, sofern die eingesetzte Hardware, auf der sich die CA-Schlüssel befinden, dies unterstützt, ausschließlich im Mehr-Augen-Prinzip durchgeführt. Der Zugriff auf diese Backups (inkl. Rücksicherung) ist nur im Mehr-Augen-Prinzip möglich. Dabei dürfen nur Verschlüsselungsalgorithmen und Algorithmusparameter gleichwertiger oder höherer Stärke benutzt werden, wie bei der Erstellung.

6.1.2. Auslieferung der privaten Schlüssel für Zertifikatsteilnehmer

Die privaten Schlüssel von Fernsignaturdiensten bzw. Fernsiegeldiensten werden ausschließlich in einem QSCD erzeugt und gespeichert und nicht an die Zertifikatsinhaber ausgeliefert. Private Schlüssel werden bei SIGN8 Token durch den Zertifikatsteilnehmer auf der USB-Stick QSCD oder Smartcard QSCD erzeugt und gespeichert.

6.1.3. Auslieferung der öffentlichen Schlüssel an die CA

Der öffentliche Schlüssel wird im Rahmen der Zertifikatserstellung verschlüsselt an die CA übertragen.

6.1.4. Auslieferung der öffentlichen CA-Schlüssel

Die CA-Zertifikate, welche die dazugehörigen öffentlichen CA-Schlüssel beinhalten, werden in der nationalen Trusted List, welche durch die zuständige Aufsichtsbehörde verwaltet wird, und somit auch in der EU Trusted List veröffentlicht. Darüber hinaus werden alle CA-Zertifikate nach ihrer Erstellung auf der Website des VDA veröffentlicht.

6.1.5. Schlüssellängen

Die QSCDs unterstützt Verschlüsselungsalgorithmen und Schlüssellängen, die der angemessenen Sicherheitsstufe entspricht, welche den beim Systementwurf identifizierten Sicherheitsbedarf erfüllt und richten sich nach ETSI TS 119 312 und ETSI EN 319 411-2.

Zurzeit werden für die Root- und CA-Zertifikate RSA-Schlüssel mit einer Länge von 4096 Bit verwendet. Für die Endanwenderzertifikate werden ECC-Schlüssel mit einer Länge von mindestens 256 Bit, oder RSA-Schlüssel mit einer Länge von 4096 Bit verwendet.

6.1.6. Schlüsselparameter und Qualitätskontrolle der Parameter

Die Schlüsselalgorithmen und -längen richten sich nach den gesetzlichen Regelungen und werden so gewählt, dass sie während der Nutzungsdauer des Unterzeichnerzertifikats standhalten können. Die Einhaltung der Vorgaben wird kontinuierlich von einer dafür verantwortlichen Person geprüft. Sollten die Schlüsselalgorithmen und -längen nicht mehr geeignet sein, werden diese Schlüssel sofort gewechselt.

6.1.7. Schlüsselverwendung

Alle Vertrauensdienste 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 VDA 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 Signaturen und Siegel verwendet werden.

Gemäß Artikel 26 (c), (d) eIDAS-Verordnung wird eine elektronische Signatur unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann. Der Signaturvorgang 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 ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Gemäß Artikel 36 (c), (d) eIDAS-Verordnung wird ein elektronisches Siegel unter Verwendung von elektronischen Siegelerstellungsdaten erstellt, die der Siegelersteller mit einem hohen Maß an Vertrauen unter seiner Kontrolle zum Erstellen elektronischer Siegel verwenden kann. Der Siegelvorgang muss durch den Unterzeichner zugestimmt werden. Die Zustimmung wird durch die Eingabe oder durch die Bestätigung des Authentifizierungsmittels angenommen. SIGN8 geht somit davon aus, dass der private Schlüssel eines Siegelerstellers nur unter seiner Zustimmung verwendet wird. Ein elektronisches Siegel ist so mit den Daten, auf die es sich bezieht, 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 eingesetzten kryptographischen Module entsprechen den gesetzlichen Anforderungen und Normen und werden in der gemäß der Zertifizierung der Komponenten notwendigen Umgebung betrieben (siehe Abschnitt 5.1. *Bauliche Sicherheitsmaßnahmen*). Der Zugriff auf die Komponenten ist durch technische und organisatorische Maßnahmen geschützt.

Alle QSCDs für die Nutzung der CAs werden in einem gesicherten Bereich aufbewahrt. Dadurch wird sichergestellt, dass die QSCDs nicht durch Dritte manipuliert werden können. Alle QSCDs für EE-Zertifikate des qualifizierten Fernsignatur- und Fernsiegeldienstes werden vom VDA betrieben und technisch überwacht.

Der VDA betreibt geeignete hard- und softwarebasierte Schlüsselgeneratoren, um die Qualität der in der PKI generierten Schlüssel zu sichern.

Zum Schutz der kryptographischen Geräte, während Betrieb, Transport und Lagerung werden die Hersteller-spezifischen Mechanismen/Maßnahmen verwendet.

6.2.2. Schlüsselaktivierung

Die Trennung der Benutzungskontrolle über die Schlüssel ist sichergestellt und der Zugriff auf die, sowie die Benutzung der Schlüssel werden durch angemessene Zugriffskontrollen geschützt. EE-Signierschlüssel dürfen und werden nicht benutzt, bevor sein Unterzeichner vom TW4S verknüpft wird.

Die CA-Schlüssel können nur in einem technisch erzwungenen Mehr-Augen-Prinzip unter Beteiligung von mehreren befugten Rollen aktiviert werden. Zum Schutz von Benutzer- und Arbeitsschlüsseln, werden benutzte Master-Schlüssel mindestens unter doppelter Kontrolle gesichert, gespeichert und neu geladen. Solche Master-Schlüssel dürfen nur außerhalb der QSCD in geschützter Form aufbewahrt werden.

Private Schlüssel von EE-Zertifikaten, die durch den VDA verwaltet werden, können ausschließlich nach erfolgreicher Identifizierung und Authentifizierung der Endanwender automatisiert aktiviert werden.

6.2.3. Schlüsselwiederherstellung

Im Rahmen dieses CPS werden private Schlüssel von EE-Zertifikaten ausschließlich durch den VDA verwaltet und können niemals die gesicherte Umgebung des VDA verlassen. In allen anderen Fällen wird eine Hinterlegung privater Schlüssel nicht angeboten.

6.2.4. Schlüsselbackup

Es ist ein Backup der privaten CA-Schlüssel vorhanden. Ein CA-Schlüssel-Backup erfordert für diese Tätigkeit am QSCD zwei autorisierte Personen und findet in der sicheren Umgebung des Trust Center statt. Für das Backupsystem gelten die gleichen Voraussetzungen und Sicherungsmaßnahmen wie für das Produktivsystem. Eine Wiederherstellung privater Schlüssel erfordert ebenfalls zwei autorisierte Personen. Der verschlüsselte Root CA Schlüssel wird auf einem separaten externen Medium gespeichert. Weitere Kopien der privaten CA-Schlüssel existieren nicht.

Alle privaten Schlüssel von EE-Zertifikaten des qualifizierten Fernsignatur- und Fernsiegeldienstes werden im Rahmen der Hochverfügbarkeit des SIGN8-Dienstes in verschlüsselter Form gesichert. Dabei ist das gleiche Sicherheitsniveau sichergestellt, wie bei den ursprünglichen privaten Schlüsseln. Diese gesicherten Schlüssel können ausschließlich in gleichwertige QSCDs wiederhergestellt und verwendet werden.

Die Anzahl der Backups von privaten Schlüsseln übersteigt nicht das benötigte Minimum, um eine Geschäftsfortführung sicherzustellen. Die CA darf nicht und bewahrt nicht die privaten Signierschlüssel des Subjekts in einer Weise auf, die eine Backup-Entschlüsselungsmöglichkeit ermöglicht (key escrow) und dazu führt, dass ihre Verwendung nicht unter der alleinigen Kontrolle des Unterzeichners steht.

In allen anderen Fällen wird ein Backup privater Schlüssel nicht angeboten.

6.2.5. Schlüsselarchivierung

Private Schlüssel dürfen und werden nicht archiviert.

Private Schlüssel dürfen und werden nicht geteilt.

6.2.6. Schlüsseltransfer

Ein Transfer privater CA-Schlüssel in oder aus dem QSCD erfolgt nur zu Backup- und Wiederherstellungszwecken. Ein Mehr-Augen-Prinzip wird erzwungen. Ein privater Schlüssel kann nicht unverschlüsselt exportiert/importiert werden und werden dahingehend durch Verschlüsselung geschützt beim Transfer, um ihre Vertraulichkeit und Integrität mit derselben oder einer höheren Sicherheitsstufe als innerhalb der QSCD sicherzustellen. Die zur Verschlüsselung genutzten Schlüssel sind mindestens so stark wie die zu übertragenden Schlüssel.

6.2.7. Schlüsselspeicherung

Die privaten Intermediate CA-Schlüssel und Infrastruktur- und Kontrollschlüssel liegen verschlüsselt im QSCD im Trust Center, welche nach FIPS 140-2 evaluiert ist, vor. Der verschlüsselte private Schlüssel der Root CA ist auf einem separaten externen Medium gespeichert. Die privaten Signierschlüssel der Unterzeichner liegen geschützt auf QSCDs.

6.2.8. Aktivierung privater Schlüssel

Die CA-Schlüssel und OCSP-Schlüssel können nur in einem technisch erzwungenen Mehr-Augen-Prinzip unter Beteiligung mehrerer Rollen aktiviert werden.

Private Schlüssel von EE-Zertifikaten können ausschließlich durch den Endanwender aktiviert und verwendet werden. Diese müssen vor jeder Verwendung aktiviert werden. Der Aktivierungsprozess wird in Abschnitt 4.2. *Verarbeitung des Zertifikatsantrags* genau beschrieben.

6.2.9. Deaktivierung privater Schlüssel

Private Schlüssel sind immer deaktiviert, sofern diese nicht nach Abschnitt 6.2.8. *Aktivierung privater Schlüssel* aktiviert wurden.

6.2.10. Zerstörung privater Schlüssel

Alle privaten Schlüssel werden vernichtet, wenn

- das Ende der Gültigkeit erreicht wurde,
- das zugeordnete Zertifikat widerrufen wurde,
- QSCDs außer Dienst gestellt wurden,
- der Signierschlüssel nutzlos für den Unterzeichner geworden ist,

- die Verknüpfung zwischen dem Signierschlüssel und dem Unterzeichner nach der Signiersitzung nicht aufrechterhalten wird und
- der Betrieb beendet wurde.

Die Zerstörung von privaten Schlüsseln stellt sicher, dass keine Restinformationen zur Rekonstruktion benutzt werden können. Die Löschung einzelner Schlüssel in Backups ist praktisch nicht machbar.

6.2.11. Beschreibung der kryptografischen Module

Der VDA betreibt geeignete und zertifizierte QSCDs zur Schlüsselgenerierung und Schlüsselbenutzung. Die eingesetzten QSCD sind FIPS 140-2 konform und unterstützen die für den Signaturerstellungsdienst erforderlichen Verschlüsselungsfunktionen. Der VDA überwacht den Zertifizierungsstatus der QSCDs. Sollte die Zertifizierung der QSCD zurückgezogen werden, wird dieser Umstand durch den VDA und ggf. anderen Parteien wie der Konformitätsbewertungsstelle oder der Bundesnetzagentur bewertet. Aus dieser Bewertung resultierende Maßnahmen werden entsprechend durchgeführt.

6.3. Weitere Aspekte der Verwaltung des Schlüsselpaars

6.3.1. Archivierung der öffentlichen Schlüssel

Alle ausgestellten Zertifikate werden für die gesamte Betriebszeit des VDA archiviert.

6.3.2. Gültigkeitsdauer von Schlüssel und Zertifikaten

Die Gültigkeitsdauer der CA-Schlüssel und Zertifikate ist variabel und dem Zertifikat zu entnehmen.

Die maximale Gültigkeitsdauer der Root- und CA-Zertifikate beträgt 15 Jahre. Es werden keine Zertifikate durch die CA ausgestellt, welche eine längere Gültigkeitsdauer als das ausstellende CA-Zertifikat haben.

Die Gültigkeitsdauer der OCSP-Zertifikate ist variabel und dem Zertifikat zu entnehmen.

Die Gültigkeitsdauer der EE-Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximale Gültigkeitsdauer beträgt fünf Jahre.

6.4. Aktivierungsdaten

6.4.1. Erzeugung und Installation von Aktivierungsdaten

Die manuelle Aktivierung privater Schlüssel von CA-Zertifikaten ist nur nach erfolgreicher Multifaktor-Authentifizierung sowie im Mehr-Augen-Prinzip möglich. Die Autorisierung des VDA-Personals erfolgt durch die verantwortlichen Rollen.

Die für die Aktivierung des privaten Schlüssels notwendigen Signaturerstellungsdaten werden vom Endanwender im Rahmen der Zertifikatsbeantragung und Identifizierung erzeugt und durch den VDA fest mit dem Zertifikatsinhaber verknüpft. Dabei wird ein Signierschlüssel mit nur einem Unterzeichner und nur einem Zertifikat für öffentliche Schlüssel mit einer hohen Vertrauensstufe verknüpft. Der VDA schützt die Integrität dieser Verknüpfung, durch die von der Datenbank bereitgestellten Integritätsfunktionen und den Protokolldaten. Ein Signierschlüssel ist immer nur mit einem SAD- und SAP-Mechanismus verknüpft.

6.4.2. Schutz von Aktivierungsdaten

Die Aktivierungsdaten müssen durch die entsprechende Person sicher verwahrt werden (geistige Aktivierungsdaten). Die Aktivierungsdaten werden durch physische Maßnahmen innerhalb der QSCD gesichert.

6.4.3. Weitere Aspekte der Aktivierungsdaten

Keine Angaben.

6.5. Computer-Sicherheitsmaßnahmen

6.5.1. Spezifische technische Sicherheitsanforderungen an Computer-Systeme

Alle IT-Komponenten, welche im Rahmen von SIGN8 verwendet werden, sind mittels verschiedener technischer und organisatorischer Maßnahmen gesichert, sodass diese Systeme ausschließlich für den designierten Zweck verwendet werden können.

Alle Kernsysteme sind redundant ausgelegt. Die Hardware wird auf Fehlfunktionen und Defekte überwacht und regelmäßig gewartet. Die vorgenommenen Einstellungen werden regelmäßig, automatisch überprüft, so dass Veränderungen erkannt werden. Die Funktionen der angebotenen Dienste werden mindestens alle zwei Monate überprüft. Sicherheitsrelevante Veränderungen, Fehlfunktionen oder Defekte werden nach Auftreten sofort an die zuständigen Personen weitergegeben, so dass diese angemessen reagieren können.

Alle Systeme werden in zugangsgeschützten Bereichen betrieben, so dass physische Veränderungen an den Systemen oder die Manipulation von Datenträgern ausgeschlossen sind.

Alle wichtigen Aktionen auf allen Servern werden zentral protokolliert. Die Protokolle werden verschlüsselt auf einer Datenbank innerhalb des gesicherten Bereichs des VDA gespeichert. Die erzeugten Protokolle und Logs können nach ihrer Erstellung weder gelöscht, noch verändert werden.

Der Zugang zu den Systemen des VDA wird erst nach Berufung in die entsprechende Rolle gewährt und bei der Abberufung sofort entzogen. Die Zugriffe erfolgen stets über Multifaktor-Authentifizierung und werden protokolliert.

Alle Mitarbeiter des VDA müssen die Arbeitseinweisungen der Vorgaben zur Computersicherheit einhalten. Defekte Datenträger werden nach einem sicheren Verfahren zerstört. Mitarbeiter des VDA sind gemäß den geltenden gesetzlichen Bestimmungen für ihr Handeln verantwortlich.

Es wird sichergestellt, dass sicherheitsrelevante Softwareupdates in angemessener Zeit auf den betroffenen Systemen eingespielt werden. Sollten Gründe existieren, die einem Update widersprechen, so müssen diese dokumentiert und dem Geschäftsführer des VDA übergeben werden.

6.5.2. Bewertung der Computersicherheit

Alle eingesetzten Systeme, die private Schlüssel von CA- oder EE-Zertifikaten verarbeiten, werden durch eine anerkannte Konformitätsbewertungsstelle regelmäßig geprüft und werden durch entsprechendes Monitoring stetig überwacht.

6.6. Technische Kontrolle während des Lebenszyklus

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

Bei der Entwicklung aller vom VDA oder im Auftrag des VDA durchgeführter Systementwicklungsprojekte werden Sicherheitsanforderungen im Entwurfsstadium analysiert. Die gewonnenen Erkenntnisse werden als Anforderungen bei der Entwicklung festgelegt.

6.6.2. Sicherheitsmaßnahmen beim Computermanagement

Ausschließlich autorisiertes Personal darf die VDA-Systeme administrieren. Durch ein entsprechendes Rollenkonzept ist festgelegt, unter welchen Voraussetzungen dies erlaubt ist (bspw. Mehr-Augen-Prinzip). Durch entsprechendes Monitoring können Regelverletzungen und andere Vorfälle erkannt werden.

6.6.3. Sicherheitsmaßnahmen beim Betrieb

Alle IT-Systeme, die im Rahmen von SIGN8 verwendet werden, werden überwacht. Bei Entdeckung sicherheitsrelevanter Ereignisse wird das Ereignis durch die jeweiligen verantwortlichen Rollen geprüft und bewertet. Je nach Bewertung wird das Ereignis entsprechend behandelt. Zu jedem Zeitpunkt wird sichergestellt, dass keine sensiblen Daten zugänglich gemacht werden. Darüber hinaus werden alle sicherheitsrelevanten Prozesse sowie Zugriffe der Mitarbeiter und Zugriffsversuche protokolliert. Protokolliert werden in dem Zusammenhang:

- Start und Beendigung der relevanten IT-Systeme,
- Systemabstürze,

- Ausfall von Hardware und
- Zugriffsversuche auf das PKI-System.

Alle sicherheitsrelevanten Protokollierungen bzw. Logs, insbesondere der CA-Systeme sowie der QSCDs, werden in der Art und Weise gesichert, dass eine Löschung des gesamten Logs oder auch einzelner Einträge im Log entweder nicht oder nur im Mehr-Augen-Prinzip möglich ist.

Es wird ausschließlich vertrauenswürdige Software aus gesicherten Quellen verwendet. Sobald sicherheitskritische Fehler allgemein bekannt werden, wird der Fehler in angemessener Zeit behoben bzw. werden sicherheitsrelevante Updates eingespielt. Jede Änderung an Software wird vorab in einer Testumgebung ausgiebig getestet, sodass schwerwiegende Fehler, die durch ein Update entstehen könnten, minimiert werden.

CA-Systeme werden so konfiguriert, dass für den Betrieb der CA nicht notwendige Eigenschaften entfernt oder deaktiviert werden.

Alle Daten werden redundant gesichert, so dass Datenverluste aufgrund alternder Datenträger vermieden werden.

Kapazitätsanforderungen und -auslastungen sowie Eignung der beteiligten Systeme werden überwacht und bei Bedarf angeglichen. Ausgetauschte Geräte oder obsoleete Datenträger werden derart außer Betrieb genommen und entsorgt, dass Funktionalitäts- oder Datenmissbrauch ausgeschlossen wird. Sicherheitskritische Änderungen werden durch den Sicherheitsbeauftragten geprüft. Nach Ablauf der Gültigkeit von CAs werden die privaten Schlüssel vernichtet.

Ausschließlich autorisiertes Personal darf die VDA-Systeme administrieren. Durch ein entsprechendes Rollenkonzept ist festgelegt, unter welchen Voraussetzungen dies erlaubt ist (bspw. Mehr-Augen-Prinzip). Durch entsprechendes Monitoring können Regelverletzungen und andere Vorfälle erkannt werden.

6.7. Netzwerksicherheit

Die IT-Systeme des VDA, am Standort des Rechenzentrums (Trust Center), werden durch Firewalls geschützt und sind redundant ausgelegt in Netzwerke anhand der Risikoanalyse, die funktionale, logische und physische Beziehungen berücksichtigt zwischen den IT-Systemen des VDA und deren Vertrauensdiensten. Die Anbindungen an das Internet und an andere Kommunikationsnetze sind redundant ausgelegt und verfügen über die für den Betrieb notwendige Bandbreite. Die Netzwerkkomponenten werden regelmäßig und automatisch auf Fehlfunktionen, Defekte, oder Manipulation überwacht. Zusätzlich wird die Netzwerkstruktur in regelmäßigen Abständen einem Review unterzogen. Systeme, die zur Umsetzung der Sicherheitspolitik angewendet werden, dürfen für keine anderen Funktionen verwendet werden.

Für die Administration der IT-Systeme wird ein separates Netz verwendet. Für Testumgebungen existieren ebenfalls separate Netze. Die Verbindungen und Protokolle zwischen den Segmenten sind auf das für den Funktionsumfang notwendige Minimum beschränkt. Alle anderen Verbindungen werden blockiert und die unerlaubten Zugriffe protokolliert. Die Übertragung sensibler Daten erfolgt grundsätzlich verschlüsselt. Besonders schützenswerte Kommunikationskanäle können nur aufgebaut werden, wenn sich die beiden Endpunkte gegenseitig authentisieren. Die Netzwerkumgebung und die Anbindung der Netzwerke sind hochverfügbar ausgelegt.

Die Einhaltung der Regeln wird regelmäßig überwacht.

OCSP-Relying Party

TLS channel start and end points	Server authentication	TLS version and channel encryption
Start - Client End – OCSP: http:// ocsp-q.sign8.eu	Keine (Siehe RFC 6960 Appendix A.1)	

VDA-Relying Party

TLS channel start and end points	Server authentication	TLS version and channel encryption
Start - Client: End – SIGN8: https://api.sign8.eu (SIGN8 APIs) https://auth.sign8.eu (SIGN8 OAuth) https://csc.sign8.eu (SIGN8 CSC API) https://localcertificate.sign8.eu (SIGN8 Token)	TLS RSA 2048 Bit	# TLS 1.3 TLS_AES_256_GCM_SHA384 (0x1302) TLS_CHACHA20_POLY1305_SHA256 (0x1303) TLS_AES_128_GCM_SHA256 (0x1301) # TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

		384 (0xc028) TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) TLS_RSA_WITH_AES_256_CBC_SHA (0x35) TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)
--	--	---

6.8. Zeitstempel

Zertifikate, Sperrlisten, Online-Statusprüfungen, das TW4S und andere wichtige Informationen enthalten Datums- und Zeitinformationen, die aus einer zuverlässigen, intern betriebenen Zeitquelle abgeleitet werden. Werden für die Fernsignatur- und Fernsiegeldienste von SIGN8 Zeitstempel benutzt, verwendet SIGN8 einen internen qualifizierten Zeitstempeldienst. Die Regelungen zum qualifizierten Zeitstempeldienst werden im Dokument Timestamping Policy der SIGN8 GmbH geregelt.

6.9. API-Sicherheit

Zur Verwendung der SIGN8 APIs durch einen Lizenznehmer muss sich dieser vor jedem Aufruf eines API-Endpunktes authentifizieren. Die für die Authentifizierung erforderlichen Zugangsdaten werden vom VDA zur Verfügung gestellt, oder können vom Lizenznehmer über das Kundenkonto angelegt werden. Eine Beschreibung der Authentifizierungsmethoden ist in den jeweiligen Entwicklerhandbüchern detailliert beschrieben. Ohne vorherige Authentifizierung ist kein Zugriff auf die angebotenen API-Endpunkte möglich.

Alle Endpunkte werden außerdem über TLS verschlüsselt. Weitere Details sind im Kapitel 6.7 Netzwerksicherheit dokumentiert.

7. Profile von Zertifikaten, Widerrufslisten und OCSP

7.1. Zertifikatsprofile

Qualifizierte Zertifikate für elektronische Signaturen erfüllen die im Anhang I der VO (EU) Nr. 2024/1183 festgelegten Anforderungen. Qualifizierte Zertifikate für elektronische Siegel erfüllen die im Anhang III der VO (EU) Nr. 2024/1183 festgelegten Anforderungen und unterliegen keinen weiteren zwingenden Anforderungen. Qualifizierte 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 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 Zertifikate werden im Format X.509v3 ausgegeben.

Die Zertifikatsprofile sind im [Cert Profile eIDAS] detailliert beschrieben.

7.1.1 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

7.1.2 Certificate Revocation List Profile (CRL)

Es werden keine Widerrufslisten von SIGN8 angeboten.

7.1.3 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 VDA 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 ist als VDA zuverlässig. SIGN8 ermöglicht der zuständigen Aufsichtsstelle und einer anerkannten Konformitätsbewertungsstelle die Überprüfung der Konformität nach den Vorgaben der Verordnung (EU) Nr. 2024/1183 und VO (EU) 910/2014. 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

Gemäß Artikel 20 Absatz 1 eIDAS-Verordnung wird SIGN8 als qualifizierter Vertrauensdiensteanbieter mindestens alle 24 Monate auf eigene Kosten von einer Konformitätsbewertungsstelle geprüft. Zweck dieser Prüfung ist es nachzuweisen, dass SIGN8 und die erbrachten qualifizierten Vertrauensdienste die in der eIDAS-Verordnung festgelegten Anforderungen erfüllen. SIGN8 legt der Aufsichtsstelle den entsprechenden Konformitätsbewertungsbericht innerhalb von drei Arbeitstagen nach Empfang vor.

Gemäß Artikel 20 Absatz 1 Buchstabe a eIDAS-Verordnung, informiert SIGN8 die Aufsichtsstelle mindestens einen Monat vor einer geplanten Überprüfung und erlaubt diesen auf Anfrage als Beobachter teilzunehmen.

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 Vertrauensdienste die Anforderungen der eIDAS-Verordnung erfüllen. Wird der Eindruck erweckt, dass gegen Vorschriften zum Schutz personenbezogener Daten verstoßen wurde, unterrichtet die Aufsichtsstelle unverzüglich die gemäß Artikel 51 der Verordnung (EU) Nr. 2016/679 eingerichteten zuständigen Aufsichtsbehörden.

Durch die Prüfung der Konformität mit den Vorgaben der Verordnung (EU) Nr. 2024/1183 und VO (EU) 910/2014 stellt die SIGN8 sicher, dass sie ihre Vertrauensdienste vertrauenswürdig und in einem rechtlich sicheren Rahmen anbietet. Der Zugang zu den Informationen ist im Abschnitt 2.4. *Zugang zu den Informationen* beschrieben.

8.2. Identität/Qualifikation des Prüfers

Die VDA-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 Vertrauensdienst 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 Vertrauensdienste gefährdet ist, wird gegebenenfalls der Betrieb bis zur Beseitigung der Mängel eingestellt.

Erfüllt SIGN8 eine der in der eIDAS-Verordnung 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

Der VDA nutzt das EU-Vertrauenssiegel gemäß Artikel 23 Absatz 1 und 2 eIDAS-Verordnung und Artikel 1 bis 4 Commission Implementing Regulation (EU) 2015/806, um seine qualifizierten Vertrauensdienste zu kennzeichnen.

9. Sonstige geschäftliche und rechtliche Regelungen

9.1. Preise

9.1.1. Preise für die Ausgabe von Zertifikaten

Die Gebühren für die Ausgabe und den Erhalt eines Zertifikats richten sich nach der mit dem Zertifikatsinhaber geschlossenen Vereinbarung.

9.1.2. Gebühren für den Zugriff auf Zertifikate

Es werden keine Gebühren für den Zugriff auf Zertifikate erhoben.

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

Für den Widerruf von Zertifikaten und die Abfrage von Statusinformationen werden keine Gebühren erhoben.

9.1.4. Gebühren für andere Dienstleistungen

Soweit andere Dienstleistungen angeboten werden, richten sich die Gebühren nach den Vereinbarungen mit dem Zertifikatsinhaber bzw. den jeweils geltenden AGB.

9.1.5. Kostenrückerstattungen

Es gelten die Vereinbarungen mit dem Zertifikatsinhaber bzw. die jeweiligen AGB.

9.2. Finanzielle Verantwortung

Gemäß Artikel 13 Absatz 1 eIDAS-Verordnung, unbeschadet des Artikel 13 Absatz 2 eIDAS-Verordnung und unbeschadet der Verordnung (EU) 2016/679, haften, Vertrauensdiensteanbieter für alle natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügten Schäden, die auf eine Verletzung der in der eIDAS-Verordnung festgelegten Pflichten zurückzuführen sind.

Bei einem qualifizierten Vertrauensdiensteanbieter wird von Vorsatz oder Fahrlässigkeit ausgegangen, es sei denn, der qualifizierte Vertrauensdiensteanbieter weist nach, dass der in Unterabsatz 1 des Artikel 13 eIDAS-Verordnung genannte Schaden entstanden ist, ohne dass er vorsätzlich oder fahrlässig gehandelt hat.

Gemäß Artikel 13 Absatz 2 eIDAS-Verordnung unterrichten Vertrauensdiensteanbieter ihre Kunden im Voraus hinreichend über Beschränkungen der Verwendung der von ihnen erbrachten Dienste und sind diese Beschränkungen für dritte Beteiligte ersichtlich, so haften die Vertrauensdiensteanbieter nicht für Schäden, die bei einer über diese Beschränkungen hinausgehenden Verwendung der Dienste entstanden sind.

Der VDA verfügt über die notwendigen Mittel, sowie der finanziellen Stabilität, um den Betrieb von Vertrauensdiensten ordnungsgemäß durchzuführen.

Außerdem verfügt der VDA über eine angemessene Deckungssumme bzw. Haftpflichtversicherung. Mitversichert ist die Tätigkeit nach der Regelung Artikel 24 Absatz 2 Buchstabe c) eIDAS-Verordnung in Verbindung mit § 10 VDG.

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 genannten Daten.

9.3.3. Zuständigkeiten für den Schutz vertraulicher Geschäftsdaten

Der VDA 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 VDA eingesetzten Mitarbeiter in dem gesetzlich zulässigen Rahmen zur Geheimhaltung der vertraulichen Daten verpflichtet.

9.4. Schutz von personenbezogenen Daten

Der VDA beachtet die gesetzlichen Bestimmungen zum Datenschutz.

9.4.1. Datenschutzkonzept

Der VDA verarbeitet personenbezogene Daten im Einklang mit den gesetzlichen Bestimmungen, vor allem der Regulation (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Die Datenschutzerklärung kann unter folgendem Link eingesehen werden: <https://sign8.eu/impressum-datenschutzerklaerung/>.

9.4.2. Definition von personenbezogenen Daten

Personenbezogene Daten sind gemäß Artikel 4 Abs. 1 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

9.4.3. Nicht vertrauliche Daten

Alle Informationen und Daten, die in den von dem VDA ausgegebenen Zertifikaten und in den in Abschnitt 2 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 personenbezogener Daten

Der VDA gewährleistet die Einhaltung des Datenschutzes.

Der Datenschutzbeauftragte des VDA achtet auf die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz. Er erarbeitet Datenschutzrichtlinien, steht als Ansprechpartner in Datenschutzfragen zur Verfügung und verpflichtet die Mitarbeiter des VDA oder mit dem VDA in vertraglicher Verbindung stehende Dritte mit Zugriff auf personenbezogene Daten zur Beachtung der Datenschutzrichtlinien.

9.4.5. Hinweis und Einwilligung zur Nutzung personenbezogener Daten

Bei der Antragsstellung wird der Zertifikatsinhaber darüber informiert, welche personenbezogenen Daten auf dem Zertifikat enthalten sein werden. Eine Datenerhebung bei Dritten erfolgt im Einklang mit den Vorgaben des § 8 Abs. 1 VDG sowie den sonstigen Bestimmungen des Datenschutzes. Eine Information im Sinne des Artikel 14 DSGVO erfolgt im Verlauf des Antragsverfahrens in Textform.

Bei der Antragsstellung werden personenbezogene Daten des Zertifikatnehmers im Rahmen des Identifikationsverfahrens erhoben und verarbeitet. Der Zertifikatsinhaber stimmt im Rahmen der Antragstellung der Nutzung seiner personenbezogenen Daten sowie deren Weitergabe zu, soweit dies für die Inanspruchnahme von Diensten Dritter erforderlich ist.

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

Der VDA unterliegt dem Recht der Bundesrepublik Deutschland sowie den Bestimmungen des BDSG und der DSGVO. Auskünfte über vertrauliche oder personenbezogene Daten werden den ermittelnden Behörden herausgegeben, sofern ein Gerichtsbeschluss vorliegt oder sonstige gesetzlichen Bestimmungen eine Herausgabe erfordern. Etwaige Herausgaben werden vom VDA 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 VDA

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 Zertifizierungskonzept enthält keine Zusicherungen, Garantien oder Gewährleistungen seitens des VDA.

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

Im Verhältnis zu Zertifikatsinhabern, Vertrauenden Dritten 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 Vertrauensdienste oder mindestens drei Monate im Falle einer beabsichtigten Einstellung dieser Tätigkeiten.

9.10.1. Gültigkeitsdauer des CPS

Diese 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 VDA 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 VDA oder Teile davon eingestellt werden, so wird diese Beendigung gemäß des Beendigungsplans des VDA durchgeführt. Der VDA hat zu prüfen, ob eine Übernahme des jeweiligen Dienstes durch einen anderen qualifizierten Vertrauensdiensteanbieter möglich ist. In dem Fall werden alle vom VDA ausgegebenen Zertifikate und Widerrufsinformationen für den zu beendenden Dienst in elektronischer Form an den neuen Vertrauensdiensteanbieter übergeben.

Ist eine Übernahme des Dienstes durch einen VDA ausgeschlossen, so werden alle vom VDA ausgegebenen Zertifikate und Widerrufsinformationen für den zu beendenden Dienst in elektronischer Form an die Bundesnetzagentur zur Übernahme in die Vertrauensinfrastruktur übergeben. Alle zu diesem Dienst zugehörigen Endanwenderzertifikate werden vor der Übergabe an die Bundesnetzagentur 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 VDA an Zertifikatnehmer werden an die letzte in den Unterlagen des VDA 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

9.12.3. Bedingungen für OID-Änderungen

Keine Angaben

9.13. Streitschlichtungsverfahren

Beschwerden können schriftlich bei SIGN8 GmbH, Fürstenrieder Str. 5, 80687 München oder via E-Mail (info@sign8.eu) eingereicht werden.

9.14. Anwendbares Recht

Dieses CPS unterliegt dem Recht der Bundesrepublik Deutschland sowie dem Recht der Europäischen Union.

9.15. Einhaltung geltenden Rechts

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

9.16. Sonstige Bestimmungen

9.16.1. Barrierefreiheit

Der VDA wird soweit möglich seine Endnutzerprodukte in einfacher und verständlicher Sprache zur Verfügung gestellt, im Einklang mit dem Übereinkommen der Vereinten Nationen über die Rechte von Menschen mit Behinderungen und den Anforderungen der Richtlinie (EU) Nr. 2019/882, so dass auch Personen mit funktionalen Einschränkungen, wie ältere Menschen, und gegebenenfalls Personen mit eingeschränktem Zugang zu digitalen Technologien davon profitieren können. Er wird im Rahmen seiner Möglichkeiten die Features zur Barrierefreiheit, der jeweiligen Betriebssysteme, bei seinen Endnutzerprodukten verfügbar machen.

9.16.2. Nichtdiskriminierungsklausel

Der VDA verpflichtet sich in einer fairen und nicht-diskriminierenden Art und Weise zu arbeiten und ihre Vertrauensdienste anzubieten, unabhängig von Merkmalen wie Rasse, Hautfarbe, Herkunft, Geschlecht, Religion, Alter, Behinderung oder sexueller Orientierung.

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.