Deutsche Telekom Security GmbH
Trust Center Certificate Policy

Version: 4.0

Gültig ab: 01.09.2023

Status: Freigegeben

Letztes Review: 28.08.2023

ÄNDERUNGSHISTORIE

Tabelle 1 - Änderungshistorie

Version	Stand	Änderungen / Kommentar
01.00	15.03.2021	Initialversion basierend auf [BR] 1.7.3, [NCSSR] 1.5, [EVCG] 1.7.4, [ETS401] 2.2.1, [ETS411-1] 1.2.2, [ETS411-2] 2.2.0, [ETS412-1] 1.1.1, [ETS412-2] 2.1.1, [ETS412-3] 1.1.1, [ETS412-4] 1.1.1, [ETS412-5] 2.2.3, [ETS312] 1.3.1, [TR3145] 1.1, [TR3145VS] 1.0
01.01	15.04.2021	Update: [BR] 1.7.4 *- nicht veröffentlicht -*
01.02	13.07.2021	Update: [ETS411-1] 1.3.1, [ETS412-1] 1.4.4, [ETS412-2] 2.2.1, [ETS412-3] 1.2.1, [ETS412-5] 2.3.1 *- nicht veröffentlicht -*
01.03	30.08.2021	Update: [BR] 1.7.5 - 1.7.9, [NCSSR] 1.6 - 1.7 *- nicht veröffentlicht -*
01.04	13.09.2021	Update: [EVCG] 1.7.5 - 1.7.8 *- nicht veröffentlicht -*
01.05	25.10.2021	Update: [BR] 1.8.0 *- nicht veröffentlicht -*
01.06	02.12.2021	Update: [ETS411-2] 2.4.1, [ETS412-4] 1.2.1 *- nicht veröffentlicht -*
02.00	01.03.2022	Jährliche Revision, Update: [BR] 1.8.1
03.00	24.01.2023	Jährliche Revision, Update [BR] 1.8.2 – 1.8.6, [EVCG] 1.7.9 – 1.8.0
04.00	01.09.2023	Aufnahme [SBR] 1.0.0 – 1.0.1, Update [BR] 1.8.7 – 2.0.0

INHALTSVERZEICHNIS

Änderungshistorie 2
Inhaltsverzeichnis 3
Tabellenverzeichnis 11
1 Einleitung 12
1.1 Überblick 12
1.2 Name und Kennzeichnung des Dokuments 15
1.3 PKI-Teilnehmer 15
1.3.1 Zertifizierungsstellen 15
1.3.2 Registrierungsstellen 16
1.3.3 Zertifikatsnehmer 16
1.3.4 Zertifikatsnutzer (vertrauende Dritte) 18
1.3.5 Andere Teilnehmer 18
1.4 Zertifikatsverwendung 18
1.4.1 Zulässige Verwendung von Zertifikaten 18
1.4.2 Unzulässige Verwendung von Zertifikaten 18
1.5 Verwaltung des Dokuments 18
1.5.1 Verwaltende Organisation dieses Dokuments 18
1.5.2 Ansprechpartner 18
1.5.3 Instanz für die Feststellung der Konformität eines CPS zu dieser CP 19
1.5.4 Genehmigungsverfahren dieser CP und eines CPS 19
1.6 Definitionen und Abkürzungen 19
2 Verantwortung für Veröffentlichung und Verzeichnisse 20
2.1 Verzeichnisse 20
2.2 Veröffentlichung von Informationen zu Zertifikaten 20
2.3 Zeitpunkt oder Häufigkeit von Veröffentlichungen 21
2.4 Zugang zu Verzeichnissen 21
3 Identifizierung und Authentifizierung 22
3.1 Namensregeln 22
3.1.1 Namensformen 22
3.1.2 Aussagekraft von Namen 22
3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsnehmer 22
3.1.4 Regeln zur Interpretation verschiedener Namensformen 23
3.1.5 Eindeutigkeit von Namen 23
3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen 23
3.2 Initiale Validierung der Identität 23
3.2.1 Methoden des Besitznachweises des privaten Schlüssels 24

3.2.2 Authentifizierung der Identität von Organisationen 24
3.2.3 Authentifizierung der Identität natürlicher Personen 25
3.2.4 Nicht überprüfte Informationen 26
3.2.5 Validierung der Bevollmächtigung 26
3.2.6 Kriterien für Interoperabilität 26
3.2.7 Validierung der Kontrolle über eine Domain oder IP-Adresse 27
3.2.8 Validierung der Kontrolle über eine E-Mail-Adresse 28
3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying) 28
3.3.1 Identifizierung und Authentifizierung für routinemäßige Schlüsselerneuerung 28
3.3.2 Identifizierung und Authentifizierung für Schlüsselerneuerung nach einer Sperrung 28
3.4 Identifizierung und Authentifizierung von Sperranträgen 28
4 Betriebliche Anforderungen an den Lebenszyklus von Zertifikaten 29
4.1 Zertifikatsantrag 29
4.1.1 Zertifikatsantragsberechtigte 29
4.1.2 Antragsprozess und -verantwortlichkeiten 29
4.2 Bearbeitung der Zertifikatsanträge 30
4.2.1 Durchführung der Identifizierung und Authentifizierung 30
4.2.2 Genehmigung oder Ablehnung von Zertifikatsanträgen 32
4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen 34
4.3 Zertifikatsausstellung 34
4.3.1 Aktivitäten der CA während der Zertifikatsaustellung 34
4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines Zertifikats 35
4.4 Zertifikatsannahme 35
4.4.1 Verhalten, das die Annahme eines Zertifikats bestätigt 35
4.4.2 Veröffentlichung des Zertifikats durch die TSP 35
4.4.3 Information Dritter über die Ausstellung von Zertifikaten durch die TSP 36
4.5 Schlüssel- und Zertifikatsnutzung 36
4.5.1 Nutzung des privaten Schlüssels und des Zertifikats 36
4.5.2 Nutzung des öffentlichen Schlüssels und des Zertifikats durch Dritte 36
4.6 Zertifikatserneuerung unter Beibehaltung der Schlüssel (Renewal) 36
4.6.1 Umstände für ein Renewal 36
4.6.2 Antragsberechtigte für ein Renewal 36
4.6.3 Verarbeitung von Anträgen auf Renewal 36
4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausstellung neuer Zertifikate 37
4.6.5 Verhalten, das die Annahme eines erneuerten Zertifikats bestätigt 37

4.6.6 Veröffentlichung erneuerter Zertifikate durch die TSP 37
4.6.7 Information Dritter über die Ausstellung neuer Zertifikate durch die TSP....37
4.7 Zertifikatserneuerung mit neuen Schlüsseln (Schlüsselerneuerung)....37
4.7.1 Umstände für eine Schlüsselerneuerung....37
4.7.2 Antragsberechtigte für eine Schlüsselerneuerung 37
4.7.3 Verarbeitung von Anträgen auf Schlüsselerneuerung....37
4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines erneuerten Zertifikats 38
4.7.5 Verhalten, das die Annahme eines erneuerten Zertifikats bestätigt 38
4.7.6 Veröffentlichung erneuerter Zertifikate durch die TSP 38
4.7.7 Information Dritter über die Ausstellung neuer Zertifikate durch den TSP....38
4.8 Änderung von Zertifikatsdaten....38
4.8.1 Umstände für eine Änderung von Zertifikatsdaten....38
4.8.2 Antragsberechtigte für eine Änderung von Zertifikatsdaten 38
4.8.3 Verarbeitung von Anträgen auf eine Änderung von Zertifikatsdaten....39
4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines erneuerten Zertifikats 39
4.8.5 Verhalten, das die Annahme eines geänderten Zertifikats bestätigt 39
4.8.6 Veröffentlichung geänderter Zertifikate durch die TSP 39
4.8.7 Information Dritter über die Ausstellung neuer Zertifikate durch den TSP....39
4.9 Zertifikatssperrung und Suspendierung....39
4.9.1 Sperrgründe....40
4.9.2 Berechtigte Sperrantragsteller....42
4.9.3 Ablauf einer Sperrung 43
4.9.4 Fristen zur Beantragung einer Sperrung....43
4.9.5 Fristen zur Verarbeitung von Sperranträgen durch die TSP 43
4.9.6 Anforderungen an Zertifikatsnutzer zur Prüfung von Sperrinformationen....44
4.9.7 Frequenz der Veröffentlichung von Sperrlisten....45
4.9.8 Maximale Latenzzeit von Sperrlisten....45
4.9.9 Verfügbarkeit von Online-Sperr-/Statusinformationen....45
4.9.10 Anforderungen an Online-Überprüfungsverfahren....45
4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen 45
4.9.12 Gesonderte Bedingungen bei Kompromittierung privater Schlüssel 45
4.9.13 Umstände für eine Suspendierung 45
4.9.14 Berechtigte Antragsteller für eine Suspendierung....46
4.9.15 Ablauf einer Suspendierung 46
4.9.16 Begrenzung der Suspendierungsperiode 46
4.10 Zertifikatsstatusdienste....46

4.10.1 Betriebliche Vorgaben 46
4.10.2 Verfügbarkeit 48
4.10.3 Optionale Merkmale 48
4.11 Kündigung durch den Zertifikatsnehmer 48
4.12 Schlüsselhinterlegung und Wiederherstellung 49
4.12.1 Schlüsselhinterlegungs- und Wiederherstellungsrichtlinien und -Praktiken 49
4.12.2 Richtlinien und Praktiken zur Kapselung und Wiederherstellung von Sitzungsschlüsseln 49
5 Bauliche, organisatorische und betriebliche Regelungen 50
5.1 Physikalische Maßnahmen 51
5.1.1 Standort und Bauweise 51
5.1.2 Physikalischer Zutritt 51
5.1.3 Stromversorgung und Klimatisierung 52
5.1.4 Wassereinwirkung 52
5.1.5 Brandvorsorge und Brandschutz 52
5.1.6 Aufbewahrung von Medien 52
5.1.7 Abfallentsorgung 52
5.1.8 Externe Sicherung 52
5.2 Organisatorische Maßnahmen 53
5.2.1 Vertrauenswürdige Rollen 53
5.2.2 Anzahl der für eine Aufgabe erforderlichen Personen 53
5.2.3 Identifizierung und Authentifizierung für vertrauenswürdige Rollen 53
5.2.4 Rollen, die eine Aufgabentrennung erfordern 54
5.3 Personelle Maßnahmen 55
5.3.1 Qualifikationen, Erfahrung und Freigaben 55
5.3.2 Verfahren zur Hintergrundprüfung 55
5.3.3 Schulungsanforderungen 56
5.3.4 Nachschulungsintervalle und -anforderungen 56
5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation 56
5.3.6 Sanktionen bei unbefugten Handlungen 56
5.3.7 Anforderungen an unabhängige Auftragnehmer 56
5.3.8 Dokumentation, die dem Personal zur Verfügung gestellt wird 57
5.4 Protokollierungsverfahren 57
5.4.1 Zu protokollierende Ereignisse 57
5.4.2 Häufigkeit der Log-Verarbeitung 58
5.4.3 Aufbewahrungszeitraum für Logdaten 58
5.4.4 Schutz der Audit-Protokolle 58
5.4.5 Backup-Verfahren für Audit-Protokolle 58

5.4.6 Audit-Sammelsystem 58
5.4.7 Benachrichtigung der Person, die ein Ereignis ausgelöst hat 58
5.4.8 Nutzung von Protokolldaten zur Schwachstellenprüfung 58
5.5 Aufbewahrung von Aufzeichnungen 59
5.5.1 Aufzubewahrende Aufzeichnungen 59
5.5.2 Aufbewahrungszeitraum für Aufzeichnungen 60
5.5.3 Schutz der Aufzeichnungen....60
5.5.4 Backup-Verfahren für Aufzeichnungen 61
5.5.5 Anforderungen an Zeitstempel von Datensätzen....61
5.5.6 Archivsystem (intern oder extern)....61
5.5.7 Verfahren zur Beschaffung und Überprüfung von Aufzeichnungen 61
5.6 Schlüsselwechsel....61
5.7 Kompromittierung und Notfall-Wiederherstellung....61
5.7.1 Verfahren zur Meldung und Behandlung von Vorfällen und Kompromittierungen 61
5.7.2 Wiederherstellung bei Beschädigung von Computern, Software oder Daten ...62
5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln....62
5.7.4 Geschäftsfortführung nach einem Notfall....63
5.8 Einstellung des CA oder RA Betriebes 63
6 Technische Sicherheitsmaßnahmen....65
6.1 Generierung und Installation von Schlüsselpaaren....65
6.1.1 Generierung von Schlüsselpaaren 65
6.1.2 Bereitstellung der privaten Schlüssel an die Zertifikatsnehmer....66
6.1.3 Übergabe öffentlicher Schlüssel an die TSP....67
6.1.4 Bereitstellung der öffentlichen CA-Schlüssel 68
6.1.5 Schlüssellängen 68
6.1.6 Generierung und Qualitätsprüfung öffentlicher Schlüsselparameter 69
6.1.7 Schlüsselverwendung 69
6.2 Schutz privater Schlüssel und technische Kontrollen kryptografischer Module 69
6.2.1 Standards und Kontrollen für kryptografische Module 69
6.2.2 Mehrpersonenkontrolle über private Schlüssel (n von m) 70
6.2.3 Hinterlegung privater Schlüssel....70
6.2.4 Sicherung privater Schlüssel....70
6.2.5 Archivierung privater Schlüssel 71
6.2.6 Übertragung privater Schlüssel in oder von einem kryptografischen Modul....71
6.2.7 Speicherung privater Schlüssel in kryptografischen Modulen....71
6.2.8 Methoden zur Aktivierung privater Schlüssel....71
6.2.9 Methoden zur Deaktivierung privater Schlüssel....72

6.2.10 Methoden zur Zerstörung privater Schlüssel 72
6.2.11 Bewertung kryptografischer Module 72
6.3 Andere Aspekte zur Verwaltung von Schlüsselpaaren 72
6.3.1 Archivierung des öffentlichen Schlüssels 72
6.3.2 Nutzungsdauer von Zertifikaten und Schlüsselpaaren 72
6.4 Aktivierungsdaten 73
6.4.1 Generierung und Installation von Aktivierungsdaten 73
6.4.2 Schutz der Aktivierungsdaten 73
6.4.3 Andere Aspekte der Aktivierungsdaten 73
6.5 Computer-Sicherheitskontrollen 74
6.5.1 Spezifische technische Anforderungen an die Computersicherheit 74
6.5.2 Sicherheitsbewertung von Computern 76
6.6 Technische Kontrollen des Lebenszyklus 76
6.6.1 Steuerung der Systementwicklung 76
6.6.2 Maßnahmen des Sicherheitsmanagements 76
6.6.3 Sicherheitskontrollen während des Lebenszyklus 77
6.7 Netzwerk-Sicherheitskontrollen 77
6.8 Zeitstempel 78
7 Zertifikats-, Sperrlisten- und OCSP-Profile 79
7.1 Zertifikatsprofile 79
7.1.1 Versionsnummer 79
7.1.2 Zertifikatserweiterungen 79
7.1.3 Algorithmen-OID 87
7.1.4 Namensformen 88
7.1.5 Namensbeschränkungen 91
7.1.6 OIDs der Erweiterung `certificatePolicies` 91
7.1.7 Verwendung der Erweiterung `policyConstraints` 91
7.1.8 Syntax und Semantik der `policyQualifier` 91
7.1.9 Verarbeitungssemantik für `certificatePolicies` 91
7.2 Sperrlistenprofile 92
7.2.1 Versionsnummer(n) 92
7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen 92
7.3 OCSP-Profil 93
7.3.1 Versionsnummer(n) 93
7.3.2 OCSP-Erweiterungen 93
8 Audits und andere Bewertungs- kriterien 94
8.1 Häufigkeit und Art der Prüfungen 94
8.1.1 Selbstüberprüfung 94

8.1.2 Prüfungen durch externe Auditoren 94
8.1.3 Prüfungen von Unterauftragnehmern und delegierten Dritten 94
8.2 Identität/Qualifikation der Prüfer 95
8.3 Beziehung des Prüfers zur geprüften Stelle 95
8.4 Abgedeckte Bereiche der Prüfung 96
8.5 Maßnahmen infolge von Mängeln 96
8.6 Mitteilung der Ergebnisse 97
9 Sonstige geschäftliche und rechtliche Bestimmungen 98
9.1 Entgelte 98
9.1.1 Gebühren für die Ausstellung oder Erneuerung von Zertifikaten 98
9.1.2 Gebühren für den Zertifikatszugang 98
9.1.3 Gebühren für den Zugang zu Sperr- oder Statusinformationen 98
9.1.4 Gebühren für andere Dienstleistungen 98
9.1.5 Rückerstattungsrichtlinie 98
9.2 Finanzielle Verantwortlichkeiten 98
9.2.1 Versicherungsschutz 98
9.2.2 Sonstige Vermögensgegenstände 99
9.2.3 Versicherungs- oder Garantiedeckung für Endteilnehmer 99
9.3 Vertraulichkeit von Geschäftsinformationen 99
9.3.1 Umfang an vertraulichen Informationen 99
9.3.2 Umfang an nicht vertraulichen Informationen 99
9.3.3 Verantwortung zum Schutz vertraulicher Informationen 99
9.4 Schutz von personenbezogenen Daten 99
9.4.1 Datenschutzkonzept 99
9.4.2 Als privat zu behandelnde Informationen 100
9.4.3 Nicht als privat geltende Informationen 100
9.4.4 Verantwortung für den Schutz privater Informationen 100
9.4.5 Benachrichtigung und Zustimmung zur Verwendung privater Informationen 100
9.4.6 Offenlegung im Rahmen eines Gerichts- oder Verwaltungsverfahrens 100
9.4.7 Andere Umstände der Offenlegung von Informationen 100
9.5 Urheberrecht 101
9.6 Zusicherungen und Gewährleistungen 101
9.6.1 Zusicherungen und Gewährleistungen der TSP 101
9.6.2 Zusicherungen und Gewährleistungen der RAs 103
9.6.3 Zusicherungen und Gewährleistungen der Zertifikatsnehmer 103
9.6.4 Zusicherungen und Gewährleistungen der Zertifikatsnutzer 106
9.6.5 Zusicherungen und Gewährleistungen sonstiger Teilnehmer 106
9.7 Gewährleistungsausschlüsse 107

9.8 Haftungsbeschränkungen....107
9.9 Schadensersatz....107
9.10 Laufzeit und Aufhebung dieser CP oder eines CPS....107
9.10.1 Laufzeit....107
9.10.2 Aufhebung....107
9.10.3 Auswirkungen der Beendigung und Fortführung....107
9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern....107
9.12 Änderungen an dieser CP oder einem CPS....108
9.12.1 Verfahren für Änderungen....108
9.12.2 Benachrichtigungsmechanismus und -zeitraum....108
9.12.3 Umstände, unter denen die OID geändert werden muss....109
9.13 Bestimmungen zur Beilegung von Streitigkeiten....109
9.14 Geltendes Recht....109
9.15 Einhaltung geltenden Rechts....109
9.16 Verschiedene Bestimmungen....109
9.16.1 Gesamte Vereinbarung....109
9.16.2 Zuordnung....109
9.16.3 Salvatorische Klausel....109
9.16.4 Rechtsdurchsetzung....110
9.16.5 Höhere Gewalt....110
9.17 Sonstige Bestimmungen....110
Anhang....111
Anhang A: Abkürzungen....111
Anhang B: Referenzen....114
Anhang C: Definitionen....116
Anhang D: Zertifikatsprofile....118
Anhang D1: Root-Zertifikate....118
Anhang D2: Sub-CA-Zertifikate....118
Anhang D3: OCSP-Signer-Zertifikate....119
Anhang D4: Endteilnehmer-Zertifikate....119
Anhang D4.1: TLS-Zertifikate....119
Anhang D4.2: S/MIME-Zertifikate....121
Anhang D4.3: Generische Zertifikatsprofile gemäß ETSI....122
Anhang D4.4: Zertifikatsprofile gemäß [3145]....123

TABELLENVERZEICHNIS

Tabelle 1 - Änderungshistorie....2
Tabelle 2 - Zertifikatserweiterungen....80
Tabelle 3 - Namensformen....88
Tabelle 4 - Abkürzungen....111
Tabelle 5 - Referenzen....114
Tabelle 6 - Definitionen....116

1 EINLEITUNG

1.1 Überblick

Die Deutsche Telekom Security GmbH (nachfolgend „Telekom Security“ genannt) betreibt zur Abbildung am Markt angebotener PKI-Produkte und kundenindividueller PKI-Lösungen mehrere Vertrauensdienste („Trust Services“)[1] zur Ausgabe von Zertifikaten und tritt somit als „Vertrauensdiensteanbieter“ (VDA) bzw. „Trust Service Provider“ (TSP)[1] auf.

Als TSP betreibt die Telekom Security in ihrem Trust Center verschiedene Zertifizierungsstellen („Certification Authorities“, CAs). Dabei handelt es sich sowohl um Wurzelzertifizierungsstellen („Root Certification Authorities“, Root-CAs) als auch um untergeordnete Zertifizierungsstellen („Subordinate Certification Authorities“, Sub-CAs) für die Ausgabe von Zertifikaten, sowohl für Kunden als auch Mitarbeiter des Konzerns Deutsche Telekom AG.

Darüber hinaus hat die Telekom Security dem „Verein zur Förderung eines Deutschen Forschungsnetzes e. V.“ (nachfolgend kurz „DFN“ genannt) öffentliche Sub-CA-Zertifikate ausgestellt, mit denen der DFN wiederum als eigenständiger TSP Zertifikate für die ihm angeschlossenen Institutionen ausstellt.

Hinweis: Es ist derzeit nicht geplant, weitere Sub-CA-Zertifikate an DFN oder andere, nicht mit der Deutschen Telekom verbundene Organisationen zu vergeben, es wird daher in diesem Dokument nicht mehr auf diesbezügliche Anforderungen eingegangen. Die im laufenden Betrieb einzuhaltenden Anforderungen gelten jedoch auch weiterhin für den DFN, so dass sich nachfolgend der Begriff TSP weiterhin sowohl auf die Telekom Security als auch, sofern anwendbar, auf den DFN bezieht.

Bei dem vorliegenden Dokument handelt es sich um die Zertifizierungsrichtlinie („Certificate Policy“, CP) des Trust Centers der Telekom Security. Es fasst in der Struktur des [RFC3647][2] alle relevanten Anforderungen aus den in Anhang B referenzierten Dokumenten zusammen, die von den Trust Services im Geltungsbereich dieser CP umgesetzt werden müssen.

Der Geltungsbereich dieser CP umfasst alle Trust Services der Telekom Security, über die Zertifikate unterhalb der

- öffentlichen und qualifizierten Root-CAs der Telekom Security,
- internen Root-CAs der Telekom Security, die sich zu dieser CP bekennen,
- Root-CAs des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) gemäß [TR3145]

ausgestellt werden.

Basis für diese CP sind die einschlägigen ETSI-Normen (siehe Anhang B). Die aus diesen ETSI-Normen resultierenden Anforderungen gelten grundsätzlich für alle Trust Services, die dieser CP unterliegen, inkl. der zu [TR3145] konformen Trust Services. Anforderungen der [TR3145], welche die ETSI-Anforderungen ergänzen oder ersetzen, sind entsprechend gekennzeichnet.

[1] In Anlehnung an den international etablierten Sprachgebrauch werden nachfolgend auch in der deutschen Version dieses Dokuments die englischen Fachbegriffe verwendet.

[2] Ergänzend zu den in [RFC3647#6] empfohlenen Kapiteln wurde diese CP um folgende Kapitel ergänzt

- 3.2.7: Validierung der Kontrolle über eine Domain
- 3.2.8: Validierung der Kontrolle über eine E-Mail-Adresse

Für die in diesem Dokument aufgeführten Anforderungen gilt folgende Semantik:

- Anforderungen ohne besondere Markierung gelten grundsätzlich übergreifend für alle Zertifikatstypen.
- Eingerahmte Anforderungen, die mit der Angabe eines oder mehrerer Zertifikatstypen in eckigen Klammern beginnen, gelten nur für die betroffenen Zertifikatstypen.
  Hinweis: Der Übersichtlichkeit halber wird in Aufzählungen auf Rahmen verzichtet.

Es werden in diesem Dokument folgende Zertifikatstypen unterschieden:

- [ETSI] kennzeichnet übergreifend alle Zertifikate, die gemäß [LCP], [NCP], [NCP+] oder [QCP] ausgestellt werden.
  - [LCP] kennzeichnet alle Zertifikate, die gemäß der in ETSI EN 319 411-1 [ETS411-1] definierten „Lightweight Certificate Policy“ ausgestellt werden.
    Sofern nicht explizit anders angegeben, gelten die Anforderungen von [LCP] implizit auch für [DVCP] und [OVCP].
  - [NCP] bzw. [NCP+] kennzeichnen alle Zertifikate, die gemäß der in [ETS411-1] definierten „Normalized Certificate Policy“ bzw. der „Extended Normalized Certificate Policy“ ausgestellt werden.
    Sofern nicht explizit anders angegeben, gelten die Anforderungen von [NCP] implizit auch für [NCP+], [QCP-n], [QCP-l], [QNCP-w] und [EVCP].
    Sofern nicht explizit anders angegeben, gelten die Anforderungen von [NCP+] implizit auch für [QCP-n-qscd], [QCP-l-qscd]
  - [QCP] kennzeichnet übergreifend alle EU qualifizierten Zertifikate nach [eIDAS], die gemäß der ETSI EN 319 411-2 [ETS411-2] ausgestellt werden. Im Einzelnen sind das:
  - [QCP-n] kennzeichnet alle qualifizierten Zertifikate für natürliche Personen.
    Sofern nicht explizit anders angegeben, gelten die Anforderungen von [QCP-n] implizit auch für [QCP-n-qscd].
  - [QCP-l] kennzeichnet alle qualifizierten Zertifikate für juristische Personen.
    Sofern nicht explizit anders angegeben, gelten die Anforderungen von [QCP-l] implizit auch für [QCP-l-qscd].
  - [QCP-n-qscd] kennzeichnet alle qualifizierten Zertifikate für natürliche Personen mit Nutzung des privaten Schlüssels in einer QSCD.
  - [QCP-l-qscd] kennzeichnet alle qualifizierten Zertifikate für juristische Personen mit Nutzung des privaten Schlüssels in einer QSCD.
  - [QNCP-w] kennzeichnet alle auf [TLS] und [NCP] basierenden qualifizierten Web-Server-Zertifikate.
  - [QEVCP-w] kennzeichnet alle auf [EVCP] basierenden qualifizierten Web-Server-Zertifikate.
- [TLS] kennzeichnet alle TLS-Authentisierungs-Zertifikate, die gemäß den „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“ des CA/Browser-Forums [BR] und der Root Store Policies von Microsoft [MSRP], Mozilla [MOZRP], Google [GCRP] und Apple [APRP] unterhalb der in den Root Stores integrierten öffentlichen Root-CAs der Telekom Security ausgestellt werden.
  Diese Kennzeichnung gilt, sofern nicht explizit anders angegeben, für TLS-Zertifikate die gemäß [DVCP], [OVCP], [EVCP], [QNCP-w] oder [QEVCP-w] ausgestellt werden.
  - [DVCP] kennzeichnet alle Zertifikate, die gemäß der in [ETS411-1] definierten „Domain Validation Certificate Policy“ ausgestellt werden.
  - [OVCP] kennzeichnet alle Zertifikate, die gemäß der in [ETS411-1] definierten „Organizational Validation Certificate Policy“ ausgestellt werden.
    Sofern nicht explizit anders angegeben, gelten die Anforderungen von [OVCP] implizit auch für [EVCP].

    - [EVCP] kennzeichnet alle Zertifikate, die gemäß der „CA/Browser Forum Extended Validation Certificate Guidelines“ [EVCG] sowie der in [ETS411-1] definierten „Extended Validation Certificate Policy“ ausgestellt werden.
      Sofern nicht explizit anders angegeben, gelten die Anforderungen von [EVCP] implizit auch für [QEVCP-w].
- [SMIME] kennzeichnet alle S/MIME-Zertifikate zur E-Mail-Absicherung, die gemäß den „Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates“ des CA/Browser-Forums [SBR] und der Root Store Policies von Microsoft [MSRP], Mozilla [MOZRP], Google Workspace [GWS] und Apple [APRP] unterhalb der in den Root Stores integrierten öffentlichen Root-CAs der Telekom Security ausgestellt werden.
  Diese Kennzeichnung gilt, sofern nicht explizit anders angegeben, für alle Zertifikate die gemäß [SMV], [SOV], [SSV] oder [SIV] ausgestellt werden.
  [SBR] unterscheidet bei den Zertifikaten die „Generationen“ Legacy, Multipurpose und Strict. Sofern sich Anforderungen nur auf bestimmte Generationen beziehen, sind diese dementsprechend mit [Legacy], [Multipurpose] und/oder [Strict] gekennzeichnet.
    - [SMV] kennzeichnet alle „Mailbox-validated“ Zertifikate gemäß [SBR].
    - [SOV] kennzeichnet alle „Organization-validated“ Zertifikate gemäß [SBR].
    - [SSV] kennzeichnet alle „Sponsor-validated“ Zertifikate gemäß [SBR].
    - [SIV] kennzeichnet alle „Individual-validated“ Zertifikate gemäß [SBR].
- [3145] kennzeichnet alle Zertifikate, die von der Telekom Security gemäß [TR3145] unterhalb der Root-CAs des BSI ausgestellt werden.
    - [VS-NfD] kennzeichnet alle Zertifikate, die gemäß [3145] ausgestellt werden und darüber hinaus den Anforderungen für VS-NfD gemäß der Erweiterung [TR3145VS] genügen.

Die Optionen oder Pflichten zur Umsetzung der Anforderungen werden durch die Schlüsselwörter gemäß [RFC2119] festgelegt:

- MUSS/MÜSSEN kennzeichnen eine unbedingte Verpflichtung.
- DARF/DÜRFEN NICHT kennzeichnen ein unbedingtes Verbot.
- SOLLTE/SOLLTEN kennzeichnen eine grundsätzliche Verpflichtung zur Umsetzung, auf die nur beim Vorliegen guter Gründe verzichtet werden kann.
- SOLLTE/SOLLTEN NICHT kennzeichnen ein grundsätzliches Verbot, es sei denn, dass gute Gründe zur Umsetzung vorliegen.
- DARF/DÜRFEN kennzeichnen eine Option.

Die Trust Services MÜSSEN die Umsetzung der für sie relevanten Anforderungen dieser CP in ebenfalls nach [RFC3647] strukturierten Certification Practise Statements (CPS) beschreiben. Die CPS MÜSSEN dabei auf alle Aspekte dieser CP eingehen und alle Kapitel des [RFC3647] berücksichtigen. Nicht anwendbare Unterkapitel MÜSSEN mit „Nicht anwendbar“ gekennzeichnet werden, d.h. diese DÜRFEN NICHT leer bleiben oder entfallen.

Die Einhaltung der Anforderungen dieser CP in der jeweils aktuellen Version MUSS explizit in den CPS bestätigt werden.

[TLS] [SMIME] Sofern anwendbar MUSS die Einhaltung der jeweils aktuellen Versionen der [BR], [SBR], [NCSSR] und [EVCG] explizit in den CPS bestätigt werden und es MUSS der Link zu den Dokumenten des CA/Browser Forums (http://www.cabforum.org) aufgeführt werden. Im Falle eines Widerspruchs zwischen dieser CP oder den CPS und den [BR], [SBR] bzw. [EVCG] haben die Regelungen aus [BR], [SBR] bzw. [EVCG] Vorrang.

Die Einhaltung der Anforderungen aus den Policies der relevanten Root Stores [MSRP], [MOZRP], [GCRP], [GWS] und [APRP] MUSS in den CPS explizit bestätigt werden. Im Falle eines Widerspruchs zwischen [MOZRP] und den [BR] haben die Regelungen aus [MOZRP] Vorrang.

Die CPS MÜSSEN unter einer Creative-Commons-Lizenz (CC-BY 4.0, CC-BY-SA 4.0, CC-BY-ND 4.0, CC-0 1.0 oder neuere Versionen) veröffentlicht werden.

1.2 Name und Kennzeichnung des Dokuments

Dieses Dokument trägt den Namen „Certificate Policy des Trust Centers der Telekom Security“ und wird durch die OID 1.3.6.1.4.1.7879.13.42 gekennzeichnet. Die OID ist wie folgt zusammengesetzt:

{iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) T-Telesec (7879) PolicyIdendifier (13) Certificate Policy des Trust Centers der Telekom Security (42)}

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen

Die Telekom Security betreibt mehrere eigene öffentliche und interne Root- und Sub-CAs. Darüber hinaus stellt sie auch eigene Cross-Zertifikate aus, jedoch keine Cross-Zertifikate zu Root- oder Sub-CAs anderer TSP.

Im Geltungsbereich dieses Dokuments liegen darüber hinaus die öffentlichen Sub-CAs des DFN, welche von der Telekom Security ausgestellt wurden.

Die vollständigen Hierarchien, d.h. alle relevanten Root- und/oder Sub-CA-Zertifikate im Gültigkeitsbereich eines CPS, MÜSSEN im jeweiligen CPS aufgeführt werden.

Hinweis: Der Einfachheit halber wird nachfolgend der Begriff „CAs“ als Synonym für „Root- und Sub-CAs“ verwendet. D.h. die Anforderungen an „CAs“ beziehen sich, sofern nicht anders angegeben, sowohl auf Root- als auch auf Sub-CAs. Gleiches gilt für den Begriff „CA-Zertifikate“, welcher zudem auch Cross-Zertifikate inkludiert.

[TLS] [SMIME] Telekom Security betreibt keine technisch beschränkten Sub-CAs.

1.3.2 Registrierungsstellen

Bei den eingesetzten Registrierungsstellen („Registration Authorities“, RAs) DARF es sich sowohl um interne RAs der TSP als auch um externe RAs handeln, welche in deren Auftrag agieren. Die in diesem Dokument aufgeführten Anforderungen an die RAs MÜSSEN, sofern anwendbar, gleichermaßen für interne als auch externe RAs umgesetzt werden.

Beim Einsatz externer RAs MÜSSEN in den CPS die Strukturen, die relevanten Prozesse sowie deren Rechte und Pflichten beschrieben werden und es MÜSSEN mit diesen entsprechende vertragliche Vereinbarungen abgeschlossen werden.

Für das Management von Zertifikaten einer Organisation oder Geräten dieser Organisation oder natürlichen Personen, die in Verbindung mit dieser Organisation stehen, DÜRFEN Enterprise-RAs als besondere Ausprägung externer RAs eingesetzt werden.

Zur Einrichtung einer Enterprise-RA einer Organisation MUSS die Organisation gemäß Kap. 3.2.2 validiert werden, der Leiter der Enterprise-RA (Ansprechpartner des TSP) sowie die mit den Registrierungs- und Zertifikatsmanagement-Tätigkeiten beauftragten RA-Mitarbeiter MÜSSEN gemäß Kap. 3.2.3 identifiziert werden und deren Berechtigung, als RA-Mitarbeiter zu agieren und ggf. weitere RA-Mitarbeiter zu bevollmächtigen, MUSS gemäß Kap. 3.2.5 nachgewiesen werden. Der TSP MUSS eine Liste der bevollmächtigten RA-Mitarbeiter pflegen und der Organisation auf Anfrage bereitstellen.

[TLS] [SMIME] Die Validierung von Domain-Namen, IP-Adressen und der Autorisierung bzw. Kontrolle über eine Mailbox DARF NICHT an externe RAs übergeben werden, siehe dazu Kap. 4.2.

Eine Enterprise-RA DARF nur Zertifikate managen, bei denen der im `subjectAltName` gesetzte FQDN oder der FQDN-Anteil der im `subjectAltName` oder in `emailAddress` gesetzten E-Mail-Adresse aus dem validierten Namensraum dieser Organisation stammt.

1.3.3 Zertifikatsnehmer

Anmerkung: Aufgrund der teilweise unterschiedlichen Verwendung der Begriffe in den in Anhang B referenzierten Dokumenten, werden nachfolgend die Begriffe beschrieben, wie sie in diesem Dokument verwendet werden.

Zertifikatsnehmer im Sinne dieser CP sind natürliche Personen oder Organisationen, für die ein Zertifikat ausgestellt wird und die durch Akzeptanz der Nutzungsbedingungen rechtlich gebunden sind. Ein Zertifikatsnehmer kann auch gleichzeitig das Subjekt eines Zertifikats und/oder der Antragsteller sein.

Organisationen im Sinne dieser CP sind juristische Personen oder organisatorische Einheiten[3], die in Verbindung mit einer juristischen Person identifiziert werden.

[3] organisatorische Einheiten, die in Verbindung mit einer juristischen Person identifiziert werden, werden nachfolgend unter dem Begriff „Organisation“ subsummiert, sofern nicht explizit anders aufgeführt

Organisationen im Geltungsbereich dieser CP können sein:

- Private Organisationen („Private Organizations“): Nichtstaatliche juristische Personen, deren Existenz durch eine Anmeldung bei oder einen Akt der Gründungsbehörde oder einer gleichwertigen Stelle begründet wurde.
- Öffentliche Organisation („Government Entities“): Von einer Regierung betriebene juristische Person, Behörde, Abteilung oder andere damit verbundene Organisationseinheiten.
- Nicht-gewerbliche Organisationen („Non-commercial Entities“): Internationale Organisationen, die im Rahmen einer Charta, eines Abkommens, einer Konvention oder eines gleichwertigen Instruments geschaffen wurden, welches von oder im Namen von mehr als einer Regierung eines Landes unterzeichnet wurde.
- Sonstige gewerbliche Organisationen („Business Entities“): Organisationen, die nicht zu den zuvor genannten Organisationstypen zählen.

Subjekt eines Zertifikats im Sinne dieser CP ist der im Zertifikat in den Attributen des `subjectDN` oder der Erweiterung `subjectAltName` benannte Anwender des privaten Schlüssels, der zu dem im Zertifikat aufgeführten öffentlichen Schlüssel korrespondiert.

Subjekte im Geltungsbereich dieser CP können

- natürliche Personen oder
- natürliche Personen, die in Verbindung mit einer Organisation identifiziert werden oder
- Organisationen oder
- Geräte[4], die von oder im Namen einer natürlichen oder juristischen Person betrieben werden.

sein.

Die Zertifikatsnehmer und Subjekte im Gültigkeitsbereich eines CPS MÜSSEN im jeweiligen CPS aufgeführt werden.

Antragsteller im Sinne dieser CP sind die Personen, welche die Anträge beim Trust Service einreichen. Es handelt sich dabei immer um natürliche Personen, die

- der Zertifikatsnehmer und/oder das Subjekt selbst,
- ein Vertretungsberechtigter des Zertifikatsnehmers (im Falle einer Organisation) oder
- eine andere, vom Zertifikatsnehmer beauftragte Person

sein können.

[EVCP] Zertifikatsnehmer DÜRFEN ausschließlich o.g. Organisationen sein.

Ergänzend zum Antragsteller MÜSSEN folgende Rollen implementiert werden:

- **Antragsunterzeichner**: Eine natürliche Person, die ausdrücklich befugt ist, den Zertifikatsnehmer zu vertreten und in dessen Namen Zertifikatsanträge zu unterzeichnen.
- **Antragsgenehmiger**: Eine natürliche Person, die ausdrücklich befugt ist, den Zertifikatsnehmer zu vertreten, und in dessen Namen Zertifikatsanträge zu genehmigen.

Es DARF eine Person mit mehreren der aufgeführten Rollen betraut werden und die Rollen DÜRFEN mit mehreren Personen besetzt werden.

[4] der Begriff „Geräte“ subsummiert nachfolgend auch Systeme, Funktionen und IT-Prozesse, sofern nicht explizit anders aufgeführt

1.3.4 Zertifikatsnutzer (vertrauende Dritte)

Keine Vorgabe.

1.3.5 Andere Teilnehmer

Keine Vorgabe.

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

Die zugelassenen Verwendungszwecke der Zertifikate MÜSSEN in den CPS, den Nutzungsbedingungen und, sofern anwendbar, den PKI Disclosure Statements (PDS) beschrieben werden.

1.4.2 Unzulässige Verwendung von Zertifikaten

Die unzulässigen Verwendungszwecke der Zertifikate MÜSSEN in den CPS, den Nutzungsbedingungen und, sofern anwendbar, den PDS beschrieben werden.

[EVCP] Die Zertifikate DÜRFEN NICHT für andere Zwecke als die TLS-Serverauthentifizierung von Web-Servern genutzt werden.

1.5 Verwaltung des Dokuments

1.5.1 Verwaltende Organisation dieses Dokuments

Das Dokument wird verwaltet von:

Deutsche Telekom Security GmbH
Trust Center & ID-Security
Untere Industriestraße 20
57250 Netphen, Deutschland

1.5.2 Ansprechpartner

Ansprechpartner für diese CP ist das PKI Compliance Management des Trust Centers, welches per E-Mail unter trustcenter-roots@telekom.de zu erreichen ist.

[TLS] [SMIME] Zur Meldung einer vermuteten Kompromittierung eines Schlüssels, eines Missbrauchs oder anderer Arten von Betrug oder unangemessenem Verhalten MÜSSEN klare Prozesse festgelegt werden. Diese MÜSSEN sowohl auf den öffentlichen Web-Seiten der TSP als auch in den CPS in Kap. 1.5.2 beschrieben bzw. veröffentlicht werden.

[VS-NfD] Ansprechpartner sind der Informationssicherheitsbeauftragte des Trust Centers sowie dessen Vertreter, welche per E-Mail unter FMB-ISMS-trustcenter@telekom.de zu erreichen sind.

1.5.3 Instanz für die Feststellung der Konformität eines CPS zu dieser CP

Zuständig für die Feststellung der Konformität eines CPS zu dieser CP ist das PKI Compliance Management des Trust Centers, Kontakte siehe Kap. 1.5.2.

1.5.4 Genehmigungsverfahren dieser CP und eines CPS

Neue Versionen dieser CP MÜSSEN von der Leitung des Trust Centers freigegeben werden.

Neue Versionen eines CPS, welche auf dieser CP basieren, MÜSSEN zunächst zur Feststellung der Konformität zu dieser CP durch das PKI Compliance Management des Trust Centers geprüft und danach von der Leitung des Trust Centers freigegen werden.

1.6 Definitionen und Abkürzungen

Definitionen, Abkürzungen und Referenzen sind im Anhang dieses Dokuments aufgeführt:

- Anhang A: Abkürzungen
- Anhang B: Referenzen
- Anhang C: Definitionen

2 VERANTWORTUNG FÜR VERÖFFENTLICHUNG UND VERZEICHNISSE

2.1 Verzeichnisse

In den CPS MUSS beschrieben werden, wer welche Verzeichnisse mit Informationen zu den ausgestellten Zertifikaten betreibt.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Die jeweils gültige Version dieses Dokuments sowie die relevanten abgelösten Versionen werden auf den Webseiten des Trust Centers der Telekom Security unter folgender Adresse veröffentlicht: https://www.telesec.de/de/service/downloads/pki-repository/

Zu jedem Trust Service MÜSSEN mindestens

- die Nutzungsbedingungen in einer allgemein verständlichen Sprache,
- die CPS,
- die CA-Zertifikate sowie
- die Statusinformationen gemäß Kap. 4.9 und 4.10 zu allen ausgestellten und noch nicht abgelaufenen Zertifikaten

über geeignete Online-Services, welche rund um die Uhr erreichbar sind, veröffentlicht werden.

Nutzungsbedingungen, CPS und CA-Zertifikate SOLLTEN, sofern nicht anders angegeben, im o.g. PKI-Repository veröffentlicht werden.

Nutzungsbedingungen und CPS MÜSSEN versioniert und mit Gültigkeitsdaten versehen sein, damit diese den ausgestellten Zertifikaten leicht erkennbar zugordnet werden können.

Darüber hinaus DÜRFEN mit Zustimmung der Zertifikatsnehmer deren Zertifikate veröffentlicht werden (siehe Kap. 4.4.2).

[TLS] Alle ausgestellten Zertifikate oder alternativ alle „Pre-Zertifikate“ (siehe Kap. 4.3.1), inkl. mindestens aller Sub-CA-Zertifikate (Root-CA optional) aus dessen Kette, MÜSSEN in einer hinreichenden Anzahl von „Certificate Transparency Logs“ (CTLogs) veröffentlicht werden. Bzgl. der Anzahl der CTLogs siehe Kap. 7.1.2 (40).

Zu jedem öffentlichen Root-Zertifikat, unterhalb dessen TLS-Serverzertifikate ausgestellt werden, MÜSSEN Test-Webseiten bereitgestellt werden, die mit TLS-Serverzertifikaten ausgestattet sind, welche bis zu der jeweiligen Root verkettet sind. Dabei MÜSSEN jeweils Webseiten mit einem gültigen, einem abgelaufenen und einem gesperrten Zertifikat bereitgestellt werden.

Sollten unterhalb einer öffentlichen Root auch TLS-Serverzertifikate gemäß [EVCG] ausgestellt werden, so MÜSSEN mindestens die o.g. Testwebseiten bereitgestellt werden, welche mit TLS-Serverzertifikaten gemäß [EVCG] ausgestattet sind.

[TLS] [SMIME] CPS und Audit-Bescheinigungen MÜSSEN (auch) in englischer Sprache veröffentlicht werden. Die übersetzten CPS MÜSSEN dabei die gleiche Versionsnummer haben wie die originalen CPS und DÜRFEN inhaltlich NICHT wesentlich von diesen abweichen. Für jedes CPS MUSS festgelegt werden, welche Version maßgeblich in Streitfällen ist.

Informationen zu allen CA-Zertifikaten MÜSSEN in der „Common CA Database“ (CCADB) gemäß der CCADB-Policy (siehe https://www.ccadb.org) veröffentlicht und aktuell gehalten werden.

Die gesamte Historie aller mit einer Root- bzw. den darunterliegenden Sub-CAs verbundenen CPS MUSS über die offiziellen Webseiten der TSP über die gesamte Zeit, in der eine Root-CA in den o.g. Root-Stores als vertrauenswürdig inkludiert ist, veröffentlicht werden.

[QCP] Zu jedem Trust Service MUSS darüber hinaus ein „PKI Disclosure Statements“ (PDS) in der Struktur gemäß des Anhang A der [ETS411-1] veröffentlicht werden. In den PDS MUSS darauf hingewiesen werden, dass der Vertrauensanker für die Validierung eines Zertifikats im Attribut `ServiceDigitalIdentity` des Eintrags des Trust Service in der Trusted List angegeben sein muss.

Von den qualifizierten Vertrauensdiensten DARF das EU-Vertrauenssiegel verwendet werden.

2.3 Zeitpunkt oder Häufigkeit von Veröffentlichungen

Neue Versionen dieser CP und der auf dieser CP basierenden CPS MÜSSEN vor Inkrafttreten veröffentlicht werden.

[TLS] [SMIME] Neue Root-CA-Zertifikate MÜSSEN spätestens bei Beantragung einer Root-Inklusion bei einer der in Kap. 1.1 aufgeführten Root-Programme veröffentlicht werden.

Neue Sub-CA-Zertifikate unterhalb der in den o.g. Root-Programmen inkludierten Root-CAs MÜSSEN vor Ihrer Inbetriebnahme, spätestens jedoch 7 Tage nach ihrer Ausstellung veröffentlicht werden.

Audit-Bescheinigungen MÜSSEN spätestens 7 Tage nach ihrer Ausstellung veröffentlicht werden.

Die Zeitpunkte bzw. Häufigkeiten der in Kap. 2.2 aufgeführten Veröffentlichungen MÜSSEN in den CPS beschrieben werden.

2.4 Zugang zu Verzeichnissen

Verzeichnisse MÜSSEN für lesenden Zugriff öffentlich verfügbar sein und MÜSSEN vor unbefugter Manipulation sowie Datenverlust geschützt sein.

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Namensregeln

3.1.1 Namensformen

In allen Zertifikaten MÜSSEN die Namen des Subjekts in Form eines Distinguished Names in die Attribute des `subjectDN` gemäß [X500] aufgenommen werden, siehe dazu Kap. 7.1.4.

In Abhängigkeit vom Zertifikatstyp MÜSSEN darüber hinaus ggf. Anforderungen an die Aufnahme von Namensbestandteilen in die Erweiterung `subjectAltName` berücksichtigt werden, siehe dazu Kap. 7.1.2.

[DVCP] Der `subjectDN` DARF auch weggelassen werden.

3.1.2 Aussagekraft von Namen

Zu Testzwecken ausgestellte Zertifikate MÜSSEN eindeutig als solche im `subjectDN` gekennzeichnet werden.

[ETSI] `commonName` in Sub-CA-Zertifikaten MÜSSEN einen gebräuchlichen Namen des TSP (nicht unbedingt der vollständige registrierte Name) beinhalten und in einer für den Markt des TSP gebräuchlichen Sprache gewählt werden. In Zertifikaten für natürliche Personen MÜSSEN die Attribute `commonName`, `surName` und `givenName`, sofern gesetzt, den Namen der Person sinnvoll abbilden. Bei Personen mit mehreren Vornamen MUSS mindestens ein Vorname angegeben werden, weitere Vornamen DÜRFEN in der von der Person gewünschten Reihenfolge angegeben werden. Gebräuchliche Abkürzungen DÜRFEN verwendet werden. Zeichen mit Akzenten oder Umlaute DÜRFEN durch entsprechende ASCII-Zeichen ersetzt werden. Bei Personen mit einem einzigen gesetzlichen Namen MUSS dieser in `surName` angegeben werden. In Zertifikaten für natürliche Personen in Verbindung mit einer Organisation MÜSSEN die Attribute `organizationName`, `organizationalUnitName` und `organization-Identifier`, sofern gesetzt, die Organisation widerspiegeln. In Zertifikaten für Organisationen MÜSSEN die Attribute `organizationName` und `organizationalUnitName`, sofern gesetzt, den vollständigen Namen der Organisation bzw. der Organisationseinheit enthalten. Es DÜRFEN gebräuchliche und unmissverständliche Abkürzungen verwendet werden, oder, um die maximale Länge von 64 Zeichen nicht zu überschreiten, auch unkritische Namensbestandteile weggelassen werden, sofern der Name noch unmissverständlich erkennbar ist. Für geografische Angaben in `localityName` oder `stateOrProvinceName` DÜRFEN Endonyme oder Exonyme verwendet werden, es SOLLTEN jedoch NICHT veraltete Namen verwendet werden.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsnehmer

Keine Vorgabe.

[TLS] Onion Domain Names DÜRFEN NICHT gesetzt werden.

[SSV] [SIV] Falls ein Pseudonym verwendet wird, MUSS hierfür eine eindeutige Kennung des TSP oder sofern anwendbar, eine innerhalb der Organisation eindeutige Kennung einer Enterprise-RA gesetzt werden.

Die Möglichkeiten zur Nutzung von Pseudonymen MÜSSEN in den CPS beschrieben werden.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Keine Vorgabe.

3.1.5 Eindeutigkeit von Namen

Die `subjectDN` aller von einer CA ausgestellten Zertifikate MÜSSEN eindeutig und jeweils einem Zertifikatsnehmer zugeordnet sein. Für einen Zertifikatsnehmer DÜRFEN aber mehrere Zertifikate mit gleichem `subjectDN` ausgestellt werden.

[DVCP] Ausgenommen hiervon ist der `subjectDN` in Domain-validierten Zertifikaten. Hier DARF ein `subjectDN` auch einem anderen Zertifikatsnehmer zugeordnet werden, wenn dieser sein rechtmäßiges Eigentumsrecht an der Domain nachgewiesen hat.

3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen

Keine Vorgabe.

[TLS] Marken- oder Handelsnamen DÜRFEN NICHT in den `subjectDN` von Zertifikaten aufgenommen werden, die von der Telekom Security ausgestellt werden.

3.2 Initiale Validierung der Identität

Zur initialen Validierung der Identität einer natürlichen Person oder einer Organisation MÜSSEN entweder direkte Nachweise oder Bescheinigungen von angemessenen und autorisierten Quellen verwendet werden.

Nachweise DÜRFEN in Papierform oder elektronisch übermittelt werden.

Die Authentizität der bereitgestellten Nachweise MUSS, soweit möglich, auf Änderungen und Fälschungen hin geprüft werden.

Nur die für die Verifizierung der Identität notwendigen Nachweise DÜRFEN verlangt werden. Antragsteller SOLLTEN darauf hingewiesen werden, nicht erforderliche Informationen in den eingereichten Nachweisen unkenntlich zu machen (z.B. nicht benötigte Datenfelder in Ausweiskopien).

Die von den Zertifikatsnehmern und ggf. davon abweichenden Antragstellern erfassten Informationen sowie deren Validierung MÜSSEN in den CPS beschrieben werden.

3.2.1 Methoden des Besitznachweises des privaten Schlüssels

Keine Vorgabe.

[TLS] Als Besitznachweis des privaten Schlüssels MUSS im Rahmen der Antragstellung eine elektronische Zertifikatsanforderung im PKCS#10-Format („Certificate Signing Request“, CSR) übergeben werden, welche mindestens eine(n) in das Zertifikat aufzunehmenden Domain Namen oder IP-Adresse enthält.

[3145] Falls die Schlüssel vom Zertifikatsnehmer generiert werden, MÜSSEN mindestens der öffentliche Schlüssel und die `subjectDN`-Attribute mit dem privaten Schlüssel signiert sein.

3.2.2 Authentifizierung der Identität von Organisationen

Die Methoden zur Authentifizierung der Identität von Organisationen MÜSSEN in den CPS beschrieben werden.

Zur Überprüfung des Namens und der Anschrift einer Organisation MUSS eine der folgenden Varianten genutzt werden:

- **QGIS** (Qualified Government Information Source): Prüfung der Daten gegen amtliche Register wie z.B. Handels- oder Vereinsregister, Stiftungsverzeichnisse etc.
- **QIIS** (Qualified Independent Information Source): Prüfung der Daten gegen Datenbestände von unabhängigen Dritten, welche als zuverlässige Datenquellen angesehen werden, z.B. „Dun&Bradstreet“, "GLEIF", etc.
- **VPL** (Verified Professional Letter): Prüfung der Daten gegen eine schriftliche Bescheinigung der Korrektheit der Daten durch einen vertrauenswürdigen Dritten (z.B. Notar, Rechtsanwalt, Wirtschaftsprüfer).
  Bei einer Bestätigung der Korrektheit der Daten mittels VPL MUSS dem VPL, sofern anwendbar, eine Kopie der betreffenden Belege beigefügt werden. Die Authentizität des VPL MUSS mittels Nachfrage über einen verifizierten Kommunikationskanal geprüft werden, sofern die Bescheinigung kein notarielles Siegel oder vergleichbare Merkmale enthält.
- **VDA-Ident**: Prüfung der Daten durch eine Vorort-Besichtigung eines autorisierten Vertreters des TSP.
- **Amtliche Beglaubigung**: Bescheinigung der Korrektheit der Daten durch eine amtliche Beglaubigung. Bei Öffentlichen Organisationen MUSS die Beglaubigung durch die Organisation selbst oder einer ihr übergeordneten Organisation erfolgen.
- **QSeal**: Verifizierung eines qualifizierten elektronischen Siegels der zu identifizierenden Organisation mittels dessen qualifiziertem Siegel-Zertifikat.
  Hinweis: Das zur Prüfung verwendete Siegelzertifikat DARF NICHT selbst auf der Grundlage einer Überprüfung eines QSeal dieser Organisation ausgestellt worden sein (Vermeidung von mehrfach aufeinanderfolgenden Identifikationen mittels QSeal).

Darüber hinaus DÜRFEN weitere, von einer Konformitätsbewertungsstelle als gleichwertig bestätigte und auf nationaler Ebene anerkannte Methoden verwendet werden.

Über die vom TSP verwendeten QGIS MÜSSEN Listen mit ausreichenden Informationen, wie z.B. Name, Gerichtsbarkeit und Website der QGIS online auf eine geeignete und leicht zugängliche Art und Weise inkl. einer Versionshistorie veröffentlicht werden. Die Veröffentlichung dieser Informationen MUSS in den CPS in Kap. 3.2 beschrieben werden.

[EVCP] Diese Liste MUSS die zugelassenen Werte zu den nachfolgend aufgeführten und in die Zertifikate aufzunehmenden Attributen enthalten:

- `jurisdictionOfIncorporationLocalityName (1.3.6.1.4.1.311.60.2.1.1)`
- `jurisdictionOfIncorporationStateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2)`
- `jursidictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3)`

[SOV] [SSV] Die eindeutige Registrierungsnummer einer Organisation MUSS mittels QGIS oder GLEIF validiert werden.

[NCP] Zur Authentifizierung der Identität einer Organisation MUSS ergänzend zu den oben aufgeführten Methoden der Antragsteller gemäß einer der in Kap. 3.2.3 aufgeführten Methoden für [NCP] identifiziert werden. Darüber hinaus MUSS dessen Bevollmächtigung gemäß Kap. 3.2.5 geprüft werden, wenn es sich bei dem Antragsteller nicht um einen direkt Vertretungsberechtigten der Organisation handelt.

[EVCP] Zur Authentifizierung der Identität einer Organisation MÜSSEN QGIS, VPL oder amtliche Beglaubigungen verwendet werden.

Darüber hinaus gelten die o.g. Anforderungen zur Identifizierung und ggf. Autorisierung des Antragstellers gemäß [NCP]. Sofern es sich bei der Organisation um den Typ „Business Entity“ handelt, MUSS der Antrag vom Hauptverantwortlichen der Organisation gestellt und dieser wie oben beschrieben identifiziert werden.

3.2.3 Authentifizierung der Identität natürlicher Personen

Die Methoden zur Authentifizierung der Identität natürlicher Personen MÜSSEN in den CPS beschrieben werden.

Zur Überprüfung der Identität einer natürlichen Person MUSS eine der folgenden Methoden genutzt werden:

- **VDA-Ident**: Überprüfung der Identität einer Person anhand eines amtlichen Ausweises durch den TSP oder eine RA.
  Die Überprüfung DARF persönlich oder mittels Videoverfahren erfolgen und MUSS folgende Aspekte berücksichtigen:
  - Prüfung der Echtheit des Ausweisdokuments
  - visueller Abgleich des Ausweisdokuments mit der zu identifizierenden Person
  - Bei Verwendung eines Videoverfahrens: Prüfung, dass die Präsentation tatsächlich live erfolgt

  Automatisierte Prozesse und Tools DÜRFEN verwendet werden, sofern die Einhaltung der o.g. Anforderungen sichergestellt ist.
- **PostIdent**: Überprüfung der Identität einer Person durch die Deutsche Post gemäß [eIDAS#24]
- **eID**: Überprüfung der Identität einer Person anhand einer Online-Identifizierung gemäß [eIDAS#24]

- **VPL**: (Verified Professional Letter): Prüfung der Daten gegen eine schriftliche Bescheinigung der Korrektheit der Daten durch einen vertrauenswürdigen Dritten (z.B. Notar, Rechtsanwalt, Wirtschaftsprüfer).
  Die Bescheinigung MUSS, sofern anwendbar, eine Kopie relevanter Unterlagen enthalten. Die Authentizität der Bescheinigung MUSS mittels Nachfrage über einen verifizierten Kommunikationskanal geprüft werden, sofern die Bescheinigung kein notarielles Siegel oder vergleichbare Merkmale enthält.
- **QES**: Überprüfung der Identität einer Person mittels Prüfung einer im Rahmen der Antragstellung oder Identifizierung von dieser Person erzeugten qualifizierten elektronischen Signatur. Erforderliche Identitätsattribute, die nicht aus dem zu prüfenden Signaturzertifikat hervorgehen, MÜSSEN auf geeignete Art und Weise anderweitig eingeholt und geprüft werden.
  Hinweis: Das zur Prüfung verwendete Signaturzertifikat DARF NICHT selbst auf der Grundlage einer Überprüfung einer QES dieser Person ausgestellt worden sein (Vermeidung von mehrfach aufeinanderfolgenden Identifikationen mittels QES).

Darüber hinaus DÜRFEN weitere, von einer Konformitätsbewertungsstelle als gleichwertig bestätigte und auf nationaler Ebene anerkannten Methoden verwendet werden.

Wenn zur Überprüfung der Identität Methoden verwendet werden, die auf Nachweisen mit befristeter Gültigkeit basieren, MUSS sichergestellt sein, dass die Nachweise zum Zeitpunkt der Prüfung noch gültig sind.

[SSV] **Enterprise-RA**: Zur Überprüfung der Identität einer natürlichen Person in Verbindung mit einer Organisation DÜRFEN alternativ die von der Organisation gepflegten Daten zum Nachweis der Identifizierung dieser Person durch die Enterprise-RA dieser Organisation genutzt werden.

3.2.4 Nicht überprüfte Informationen

Ggf. verwendete, nicht überprüfte Informationen MÜSSEN in den CPS aufgeführt werden.

3.2.5 Validierung der Bevollmächtigung

Zur Validierung einer Bevollmächtigung, Zertifikate im Namen einer natürlichen Person oder Organisation beantragen und managen zu dürfen, MUSS eine rechtsgültig unterschriebene Vollmacht von der zu vertretenden Person oder Organisation eingefordert werden:

- Bei Vertretung einer natürlichen Person, die nicht mit einer Organisation verbunden ist: eine Vollmacht der natürlichen Person
- Bei Vertretung einer Organisation oder einer natürlichen Person in Verbindung mit einer Organisation: eine Vollmacht der Organisation

[EVCP] Zur Validierung einer Bevollmächtigung, Zertifikatsanträge zu unterschreiben oder zu genehmigen, DARF alternativ auch eine Bestätigung über einen verifizierten Kommunikationskanal bei einem Vertretungsberechtigten der Organisation eingeholt werden.

3.2.6 Kriterien für Interoperabilität

Keine Vorgabe.

[TLS] [SMIME] Alle Cross-Zertifikate, in denen eine Organisation der Deutschen Telekom als Subjekt enthalten ist, MÜSSEN veröffentlicht werden.

3.2.7 Validierung der Kontrolle über eine Domain oder IP-Adresse

Keine Vorgabe.

[TLS] Jeder FQDN MUSS mithilfe einer der folgenden Methoden validiert werden:

- E-Mail, Fax, SMS oder Post an den Domain-Kontakt gemäß [BR#3.2.2.4.2],
- konstruierte E-Mail an den Domain-Kontakt gemäß [BR#3.2.2.4.4],
- DNS-Veränderung gemäß [BR#3.2.2.4.7],
- IP-Adressenprüfung gemäß [BR#3.2.2.4.8],
- Validierung des Antragstellers als Domain-Kontakt gemäß [BR#3.2.2.4.12],
- E-Mail an den DNS CAA E-Mail-Kontakt gemäß [BR#3.2.2.4.13],
- E-Mail an den DNS CAA TXT-Record-E-Mail-Kontakt gemäß [BR#3.2.2.4.14],
- Telefonanruf beim Domain-Kontakt gemäß [BR#3.2.2.4.15],
- Telefonanruf beim DNS TXT Record-Kontakt gemäß [BR#3.2.2.4.16],
- Telefonanruf beim DNS CAA-Kontakt gemäß [BR#3.2.2.4.17],
- Vereinbarte Änderung der Webseite v2 gemäß [BR#3.2.2.4.18],
- Vereinbarte Änderung der Webseite ACME gemäß [BR#3.2.2.4.19],
- TLS unter Verwendung von ALPN gemäß [BR#3.2.2.4.20].

Auf die Validierung weiterer FQDNs oder Wildcard Domain Names, welche mit den Domain Labels des validierten FQDN enden, DARF nach einer erfolgreichen Validierung eines FQDN gemäß einer der oben aufgeführten Methoden aus [BR#3.2.2.4] verzichtet werden. Hiervon ausgenommen sind Validierungen gemäß [BR#3.2.2.4.8], [BR#3.2.2.4.18], [BR#3.2.2.4.19] und [BR#3.2.2.4.20].

Für jeden Wildcard Domain-Name, der in ein Zertifikat aufgenommen werden soll, MUSS geprüft werden, dass der FQDN-Teil vom Typ "registry-controlled" oder "public suffix" ist. Zu dieser Prüfung DARF auf eine regelmäßig aktualisierte „Public-suffix-list“ (PSL) zurückgegriffen werden. Wenn eine solche PSL zur Prüfung verwendet wird, SOLLTEN nur die „ICANN Domains“ akzeptiert werden.

Die Validierung der Kontrolle über eine IP-Adresse MUSS gemäß einer der folgenden Methoden durchgeführt werden:

- Vereinbarte Änderung der Webseite gemäß [BR#3.2.2.5.1],
- E-Mail, Fax, SMS oder Post an den IP-Adress-Kontakt gemäß [BR#3.2.2.5.2],
- Rückwärtssuche nach Adressen gemäß [BR#3.2.2.5.3],
- Telefonanruf beim IOP-Adress-Kontakt gemäß [BR#3.2.2.5.5],
- ACME "http-01"-Methode für IP-Adressen gemäß [BR#3.2.2.5.6],
- ACME "tls-alpn-01"-Methode für IP-Adressen gemäß [BR#3.2.2.5.7].

Um zu verhindern, dass IP-Adressen verwendet werden, welche in anderen Ländern als dem tatsächlichen Sitz des Antragstellers vergeben wurden, SOLLTE ein Verfahren zur Überprüfung von Proxy-Servern eingeführt werden.

Die verwendeten Methoden nach [BR#3.2.2.4] bzw. [BR#3.2.2.5] inkl. eines Verweises auf das relevante Kapitel der [BR] MÜSSEN in den CPS aufgeführt werden.

3.2.8 Validierung der Kontrolle über eine E-Mail-Adresse

Keine Vorgabe.

[SMIME] Zur Verifizierung der Kontrolle des Antragstellers über die im Zertifikat referenzierten E-Mail-Adressen bzw. der Autorisierung des Antragstellers, im Namen des tatsächlichen Inhabers der E-Mail-Adressen zu handeln, MUSS ein der folgenden Methoden angewendet werden:

a) Validierung der Kontrolle des Antragstellers über den Domänen-Anteil der E-Mail-Adresse (z.B.im Fall einer Enterprise-RA)
b) Validierung der Kontrolle über jede einzelne Mailbox per Validierungs-E-Mail

Zur Validierung der Domain Namen MÜSSEN die in Kap. 3.2.7 aufgeführten Methoden verwendet werden.

Die Validierung der Kontrolle über eine Mailbox mittels Validierungs-E-Mail MUSS unter Nutzung individueller und befristet gültiger Zufallswerte gemäß [SBR#3.2.2.2] erfolgen.

Die angewandten Verifizierungsmethoden MÜSSEN in den CPS beschrieben werden.

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

3.3.1 Identifizierung und Authentifizierung für routinemäßige Schlüsselerneuerung

Es gelten die Anforderungen gemäß Kap. 3.2. Zur Validierung der Identität DÜRFEN bereits vorhandene Nachweise, unter Berücksichtigung der anwendbaren Rechtslage und der verbliebenen Gültigkeit der Nachweise (siehe Kap. 4.2.1), wiederverwendet werden.

3.3.2 Identifizierung und Authentifizierung für Schlüsselerneuerung nach einer Sperrung

Gesperrte Zertifikate DÜRFEN NICHT erneuert werden. Nach einer Sperrung MUSS ein neues Zertifikat beantragt werden und die Validierung MUSS wie bei der initialen Beantragung erfolgen.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Methoden zur Identifizierung und Authentifizierung von Sperranträgen MÜSSEN in den CPS festgelegt werden.

4 BETRIEBLICHE ANFORDERUNGEN AN DEN LEBENSZYKLUS VON ZERTIFIKATEN

Die nachfolgend aufgeführten Anforderungen MÜSSEN für alle Zertifikate umgesetzt werden, inkl. der Zertifikate, welche die TSP für sich selbst oder ihre Mitarbeiter ausstellen.

Sofern nicht explizit anders angegeben, gelten die Anforderungen für Zertifikate aller Hierarchieebenen.

4.1 Zertifikatsantrag

4.1.1 Zertifikatsantragsberechtigte

Zertifikatsantragsberechtigte sowie deren möglichen Rollen MÜSSEN in den CPS beschrieben werden.

Zur Vermeidung von Interessenskonflikten DÜRFEN die TSP NICHT selbst als Antragsteller von Endteilnehmer-Zertifikaten fungieren. Ausnahmen bilden die Organisationen, welche Registrierungstätigkeiten durchführen und sich selbst oder Personen, die in Verbindung mit dieser Organisation identifiziert werden, Zertifikate ausstellen. Die Ausnahmen MÜSSEN in den CPS beschrieben werden.

4.1.2 Antragsprozess und -verantwortlichkeiten

Antragsprozesse inkl. der zu nutzenden Schnittstellen MÜSSEN in den CPS klar beschrieben werden.

Von den Antragstellern MÜSSEN Zertifikatsanträge mit folgenden Angaben eingefordert werden:

- mindestens eine Kontaktangabe (physische Adresse, E-Mail-Adresse oder andere Angaben),
- alle in den `subjectDN` oder den `subjectAltName` aufzunehmenden Attribute,
- die Bestätigung der Kenntnisnahme und Akzeptanz der Nutzungsbedingungen,
- die Zustimmung zur Aufzeichnung der im Rahmen des Zertifikatsmanagements erfassten Daten,
- sofern anwendbar, eine Aussage bzgl. der Veröffentlichung des Zertifikats.

Ein Zertifikatsantrag DARF zur Beantragung mehrerer Zertifikate verwendet werden. Dabei MUSS jedoch sichergestellt werden, dass die Akzeptanz der Nutzungsbedingungen für jedes Zertifikat gegeben ist.

Diese Daten MÜSSEN entweder vom Antragsteller selbst bei Antragstellung bereitgestellt werden oder nach Abfrage bei vertrauenswürdigen Quellen vom Antragsteller bestätigt werden.

Hinweis: Wenn Zertifikatsnehmer und Subjekt eines Zertifikats unterschiedliche Personen oder Organisationen sind und das Subjekt des Zertifikats kein Gerät ist, MÜSSEN beide Personen/Organisationen bestimmte Teile der Nutzungsbedingungen akzeptieren, bzgl. der Details sei auf Kap. 9.6.2 verweisen.

Zertifikatsanträge DÜRFEN in elektronischer Form gestellt werden. In diesem Fall MÜSSEN die Anträge inkl. der Akzeptanz der Nutzungsbedingungen durch eine nachvollziehbare Handlung (z. B. Ankreuzen eines Kästchens im Web-Antragsformular) bestätigt oder elektronisch signiert werden.

[EVCP] Fehlende Informationen MÜSSEN vom Antragsgenehmiger oder Antragsunterzeichner bereitgestellt oder bestätigt werden.

[QCP] Elektronisch eingereichte Zertifikatsanträge SOLLTEN mindestens mit einer fortgeschrittenen elektronischen Signatur oder einem fortgeschrittenen elektronischen Siegel versehen sein.

[VS-NfD] Der Antragsprozess MUSS durch den Sicherheitsbeauftragten freigegeben werden.

4.2 Bearbeitung der Zertifikatsanträge

Zertifikatsanträge MÜSSEN auf Korrektheit, Vollständigkeit und Autorisierung geprüft werden.

Die nachfolgend aufgeführten Bearbeitungsschritte MÜSSEN von vertrauenswürdigem Personal (siehe dazu auch Kap. 5.2.1) durchgeführt werden.

Die Bearbeitung der Zertifikatsanträge oder Teile davon DÜRFEN an Externe RAs ausgelagert werden. In diesem Fall MUSS sichergestellt werden, dass der Prozess als Ganzes den Anforderungen dieser CP genügt. Die externen RAs MÜSSEN identifiziert und authentifiziert werden und der sichere Austausch der Informationen zwischen externer RA und TSP MUSS sichergestellt werden.

[TLS] Ausgenommen davon ist die Validierung über die Kontrolle einer Domain oder IP-Adresse gemäß Kap. 3.2.7, welche von den TSP selbst durchgeführt werden MUSS.

[SMIME] Ausgenommen davon ist die Validierung des Authorization Domain Name (gemäß [BR]) des Domain-Anteils der E-Mail-Adresse, welcher von den TSP selbst durchgeführt werden MUSS.

4.2.1 Durchführung der Identifizierung und Authentifizierung

Die Identität der Zertifikatsnehmer und, sofern davon abweichend, der Antragsteller, MÜSSEN zum Zeitpunkt der Registrierung gemäß der in Kap. 3.2 beschriebenen Methoden validiert werden.

Die Bevollmächtigung eines Antragstellers MUSS gemäß Kap. 3.2.5 geprüft werden, wenn der Antragsteller nicht zugleich auch der Zertifikatsnehmer ist.

Ist das Subjekt eines Zertifikats eine natürliche Person, dann MÜSSEN

- der vollständige Name der Person,
- das Geburtsdatum und der -ort oder der Verweis auf ein amtliches Ausweisdokument oder andere Attribute, welche für eine eindeutige Identifikation herangezogen werden können,

überprüft werden.

Ist das Subjekt eines Zertifikats eine natürliche Person in Verbindung mit einer Organisation, dann MÜSSEN zusätzlich

- der vollständige Name und Rechtsstand der Organisation,
- alle relevanten Registrierungsinformationen der Organisation,
- die Zugehörigkeit der natürlichen Person zur Organisation sowie
- die Bestätigung der Person und der Organisation, dass die Attribute die Organisation korrekt widerspiegeln,

überprüft werden.

Ist das Subjekt eines Zertifikats eine Organisation, dann MÜSSEN

- der vollständiger Name Organisation,
- alle relevanten Registrierungsinformationen der Organisation,
- eine national anerkannte Identitätsnummer oder andere Attribute, die verwendet werden können, um die Organisation so weit wie möglich von anderen mit demselben Namen zu unterscheiden,
- falls anwendbar, die Verbindung der Organisation zu der organisatorischen Einheit, die in Verbindung mit dieser Organisation identifiziert wird,

überprüft werden.

Ist das Subjekt eines Zertifikats ein Gerät, welches von einer natürlichen Person oder einer Organisation betrieben wird, dann MUSS zusätzlich die Kennung des Geräts (z. B. Internet Domain Name) überprüft werden.

Alle Informationen, die in einem Zertifikat enthalten sein sollen, MÜSSEN überprüft werden.

[3145] Bei der Validierung einer Identität MUSS geprüft werden, ob der Zertifikatsnehmer bereits zuvor registriert wurde. Wenn das der Fall ist, so MÜSSEN alle weiteren Zertifikate dem registrierten Zertifikatsnehmer zugeordnet werden, damit im Fall einer Suspendierung des Zertifikatsnehmers alle Zertifikate dieses Zertifikatsnehmers gemäß den Nutzungsbedingungen gleichzeitig suspendiert oder gesperrt werden können.

[TLS] [SMIME] Zur Ausstellung weiterer Zertifikate DÜRFEN durchgeführte Validierungen innerhalb folgender Zeiträume wiederverwendet werden:

- Validierungen von Daten gemäß Kap. 3.2, mit Ausnahme von Kap. 3.2.7 und 3.2.8: 825 Tage
- Validierungen gemäß Kap. 3.2.7 bzw. 3.2.8 a): 398 Tage
- Validierungen gemäß Kap. 3.2.8 b): 30 Tage

[OVCP] Die Prüfung der Authentizität eines Zertifikatsantrags MUSS über eine verifizierte Methode der Kommunikation mit einer als verbindlich angesehenen Stelle der Organisation erfolgen.

Den Organisationen MUSS die Möglichkeit geboten werden, berechtigte Personen zur Beantragung von Zertifikaten zu benennen. Wenn eine Organisation berechtigte Personen schriftlich benannt hat, DÜRFEN Zertifikatsanträge von anderen als den benannten Personen NICHT akzeptiert werden. Auf eine schriftliche Anfrage einer Organisation MUSS eine Liste der von der Organisation benannten berechtigten Personen zur Verfügung gestellt werden.

[EVCP] Die rechtliche, physische und betriebliche Existenz einer Organisation MÜSSEN im Rahmen der Validierung der Identität der Organisation gemäß Kap. 3.2.2 geprüft werden und es MUSS der Typ der Organisation festgelegt werden. Die Prüfung der rechtlichen Existenz umfasst auch, sofern anwendbar, die Prüfung bzw. Erfassung von Registrierungsnummern oder Gründungsdaten, Vertretungsberechtigungen oder Verantwortlichen sowie ggf. Beziehungen zwischen Unternehmen und Muttergesellschaften bzw. Tochtergesellschaften oder Beteiligungen. Die Prüfung der physischen und betrieblichen Existenz umfasst auch die Prüfung der Adresse der Organisation.

Des Weiteren MUSS geprüft werden, ob der Antrag von einem berechtigten Antragsunterzeichner und einem berechtigten Antragsgenehmiger unterschrieben ist. Dazu MÜSSEN

- deren Bevollmächtigung gemäß Kap. 3.2.5 geprüft werden, sofern diese nicht direkt vertretungsberechtigt sind und
- über eine verifizierte Methode der Kommunikation mit den o.g. Personen geprüft werden, dass die Unterschriften tatsächlich von diesen Personen in den zugewiesenen Rollen geleistet wurden.

Alternativ zur handschriftlichen Unterzeichnung des Antrags durch den Antragsunterzeichner und den Antragsgenehmiger DÜRFEN auch folgende Methoden akzeptiert werden:

- fortgeschrittene oder qualifizierte elektronische Signaturen der o.g. Personen
- Bestätigung durch die o.g. Personen über ein Web-Frontend, vorausgesetzt, dass diese zuvor angemessen registriert wurden und sich über ein sicheres Verfahren am Web-Frontend authentisieren

In diesen Fällen DARF auf die Bestätigung der geleisteten Unterschrift mittels verifizierter Kommunikation verzichtet werden.

Nach erfolgreicher Durchführung aller Validierungen MUSS eine sorgfältige Gegenprüfung aller durchgeführten Validierungen durch einen weiteren RA-Mitarbeiter, der nicht in die Validierungen selbst involviert war, erfolgen.

Zur Ausstellung weiterer Zertifikate DÜRFEN durchgeführte Validierungen nur innerhalb von 398 Tagen wiederverwendet werden.

[VS-NfD] Die Sicherheitsfreigabe des Zertifikatsnehmers MUSS in Bezug auf die Nutzung der PKI verifiziert werden.

4.2.2 Genehmigung oder Ablehnung von Zertifikatsanträgen

Zertifikatsanträge DÜRFEN nur nach erfolgreicher Identifizierung und Authentifizierung gemäß Kap. 4.2.1 genehmigt werden.

Wenn zu einem Antrag ein vom Zertifikatsnehmer generierter Schlüssel vorgelegt wird, MUSS der Besitz oder die Kontrolle über den privaten Schlüssel geprüft werden. Im Falle der Übergabe eines Schlüssels in Form eines PKCS#10-Requests MUSS dessen Signatur geprüft werden. Darüber hinaus MUSS geprüft werden, ob der vorgelegte Schlüssel den Anforderungen aus Kap. 6.1.5 und 6.1.6 genügt. Bei einem negativen Prüfergebnis MUSS der Antrag abgelehnt werden.

[TLS] [SMIME] Wenn in einem Antrag ein Schlüssel vorgelegt wird, dessen korrespondierender privater Schlüssel

- nachweislich mittels einer fehlerhaften Methode erzeugt wurde,
- über eine bekannte oder nachgewiesene Methode kompromittiert werden kann, z.B., wenn es sich um einen „Debian weak key“ handelt oder
- dem TSP als kompromittiert gemeldet wurde (siehe dazu auch Kap. 4.9.1)

MUSS der Antrag abgelehnt werden.

[TLS]

Innerhalb von 8 Stunden vor der Ausstellung eines Zertifikats MUSS für jeden in das Zertifikat aufzunehmenden Domain Namen geprüft werden, ob der TSP als berechtigter Aussteller in den CAA-Records wie folgt aufgeführt ist:

- Bei Anträgen zu Zertifikaten mit einem oder mehreren FQDN: im „issue“-Feld eines jeden FQDN.
- Bei Anträgen zu Zertifikaten mit Wildcards: im „issuewild“-Feld des FQDN-Teils.

Ein Zertifikat DARF auch dann ausgestellt werden, wenn die o.g. Felder leer sind.

Nach einer fehlgeschlagenen Abfrage eines CAA-Records DARF dennoch ein Zertifikat ausgestellt werden, wenn:

- der Fehler außerhalb der Infrastruktur des TSP liegt,
- die Abfrage mindestens einmal wiederholt wurde und
- die Zone der Domäne keine DNSSEC-Validierungskette zur ICANN-Root hat.

Die vom TSP akzeptierten Aussteller-Domain-Namen MÜSSEN in den CPS in Kap. 4.2 aufgeführt werden.

Wenn diese Prüfung für ein Pre-Zertifikat, welches in mindestens zwei CT-Log-Servern geloggt wurde, durchgeführt wurde, so DARF bei der Ausstellung des korrespondierenden Leaf-Zertifikats auf eine erneute Prüfung verzichtet werden.

Bei technisch beschränkten Sub-CAs DARF auf die CAA-Prüfung verzichtet werden, wenn der Verzicht auf die CAA-Prüfung explizit in dem Vertrag mit dem Zertifikatsnehmer vereinbart wurde.

Für „High-Risk-Zertifikatsanträge“ MÜSSEN zusätzlich erforderliche Prüfungen umgesetzt werden.

Darüber hinaus MUSS geprüft werden, dass sowohl die antragstellende Organisation als auch die handelnden Personen nicht in den zu berücksichtigenden Verbots- oder Sanktionslisten aufgeführt sind.

[EVCP] Anträge zu Wildcard Zertifikaten MÜSSEN abgelehnt werden.

[QCP-l-qscd] [QCP-n-qscd] Wenn in einem Antrag ein Schlüssel vorgelegt wird, von dem nicht sichergestellt ist, dass dieser von einem in einem QSCD generierten Schlüsselpaar stammt, MUSS der Antrag abgelehnt werden.

[3145] Zertifikatsanträge von suspendierten Endteilnehmern MÜSSEN abgelehnt werden.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Keine Vorgabe.

4.3 Zertifikatsausstellung

4.3.1 Aktivitäten der CA während der Zertifikatsaustellung

Die Integrität und Authentizität aller Daten MÜSSEN durch entsprechende (technische, organisatorische oder personelle) Maßnahmen sichergestellt werden.

Der Prozess der Ausstellung der Zertifikate MUSS sicher mit der zugehörigen Registrierung und mit dem vom Antragsteller übergebenen bzw. vom TSP erzeugten Schlüssel verknüpft werden.

4.3.1.1 Ausstellung von CA-Zertifikaten

CA-Zertifikate MÜSSEN in der sicheren Umgebung des Trust Centers im Rahmen einer Zeremonie ausgestellt werden. Die beteiligten Rollen sowie deren Aufgaben und Verantwortlichkeiten vor, während und nach der Zeremonie MÜSSEN festgelegt und dokumentiert sein.

Die einzelnen Schritte der Zeremonie MÜSSEN einem festgelegten Protokoll folgen und in diesem dokumentiert werden.

Die Ausstellung MUSS durch mindestens zwei vertrauenswürdige Mitarbeiter des Trust Centers erfolgen, es gelten dabei folgende Anforderungen:

- Jeder der beiden Mitarbeiter MUSS Kenntnis von nur einem Teil der zur Zertifikatsausstellung erforderlichen Aktivierungsdaten haben.
- Die beiden Mitarbeiter MÜSSEN in unterschiedlichen Rollen agieren.

Bei der Ausstellung von Sub-CA-Zertifikaten MUSS zum Nachweis der Authentizität und Integrität des Schlüssels der Hashwert des öffentlichen Schlüssels oder des CSR, der den öffentlichen Schlüssel beinhaltet, geprüft werden.

Ein interner Auditor (siehe Kap. 8.2) MUSS die Zeremonie überwachen und deren korrekte Durchführung im Protokoll bestätigen.

[TLS] [SMIME] Sowohl ein interner als auch ein qualifizierter externer Auditor (siehe Kap. 8.2) MÜSSEN die Zeremonie überwachen und deren korrekte Durchführung im Protokoll bestätigen.

4.3.1.2 Ausstellung von Endteilnehmer-Zertifikaten

Wenn die TSP die Endteilnehmer-Schlüssel generieren, MUSS die Vertraulichkeit der Schlüssel im Generierungsprozess sichergestellt werden.

[TLS] Endteilnehmer-Zertifikate MÜSSEN vor Ausstellung

- durch geeignete Lint-Tools geprüft und
- in einer hinreichend großen Anzahl von CT-Log-Servern (Certificate Transparency gemäß [RFC6962]) als „Pre-Zertifikate“ veröffentlicht

werden.

Die von den CTLog-Servern zurückgelieferten Bestätigungen mit Zeitstempeln MÜSSEN in die Zertifikate als „Embedded Signed Certificate Timestamps“ (SCT)) aufgenommen werden. Bzgl. der Anzahl der SCTs sei auf Kap. 7.1.2 verwiesen.

[3145] Wenn die Nutzung kryptografischer Token gefordert ist, MUSS

- über technische Maßnahmen sichergestellt werden, dass der gelieferte öffentliche Schlüssel korrekt dem Token und den Registrierungsdaten zugeordnet wird,
- sichergestellt werden, dass der korrekte öffentliche Schlüssel des ausgewählten Tokens ins Zertifikat übernommen wird und dass das Zertifikat auf dem richtigen Token abgelegt wird,
- sichergestellt werden, dass der personalisierte Token an den richtigen Empfänger gesendet wird,
- der Versand/die Übergabe der Token so gestaltet werden, dass ein von einem Angreifer abgefangener Token nicht verwendet werden kann, z.B. durch eine zur Nutzung des Tokens erforderliche Aktivierung, die nur durch den berechtigten Empfänger mittels Aktivierungsdaten, die ihm über einen separaten Kanal übergeben wurden, durchgeführt werden kann.

[VS-NfD] Die Vorgaben aus [VSA] zum Schutz der Schlüssel gemäß ihrer Klassifikation MÜSSEN beachtet werden.

4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines Zertifikats

Zertifikatsnehmer MÜSSEN über die Ausstellung der Zertifikate informiert werden.

Sofern anwendbar, MÜSSEN die Zertifikate den Zertifikatsnehmern in nutzbarer Form übergeben werden, ggf. auch erst zu einem späteren Zeitpunkt.

4.4 Zertifikatsannahme

4.4.1 Verhalten, das die Annahme eines Zertifikats bestätigt

Keine Vorgabe.

4.4.2 Veröffentlichung des Zertifikats durch die TSP

Zertifikate DÜRFEN mit Zustimmung des Zertifikatsnehmers veröffentlicht werden, sie DÜRFEN jedoch NICHT ohne Zustimmung veröffentlicht werden.

4.4.3 Information Dritter über die Ausstellung von Zertifikaten durch die TSP

Keine Vorgabe.

[TLS] CA-Zertifikate MÜSSEN in der CCADB, Endteilnehmer-Zertifikate bzw. die korrespondierenden Pre-Zertifikate in mehreren CT-Log-Servern veröffentlicht werden. Siehe Kap. 4.3.1.

4.5 Schlüssel- und Zertifikatsnutzung

4.5.1 Nutzung des privaten Schlüssels und des Zertifikats

Nutzungszwecke privater Schlüssel und Zertifikate MÜSSEN in den CPS beschrieben werden.

[QCP-n-qcsd] [QCP-l-qcsd] Die Nutzung des privaten Schlüssels MUSS auf die Erzeugung elektronischer Signaturen bzw. elektronischer Siegel beschränkt werden, wenn die QSCD des Zertifikatsnehmers vom TSP gemanagt wird.

4.5.2 Nutzung des öffentlichen Schlüssels und des Zertifikats durch Dritte

Dritte SOLLTEN die in den Nutzungsbedingungen aufgeführten Vorgaben zur Nutzung und Prüfung der Zertifikate und öffentlichen Schlüssel beachten.

4.6 Zertifikatserneuerung unter Beibehaltung der Schlüssel (Renewal)

4.6.1 Umstände für ein Renewal

Die Umstände und ggf. Zeiträume, unter denen ein Renewal erlaubt ist, MÜSSEN in den CPS festgelegt werden. Dabei MÜSSEN die Aspekte der Schwächung der Schlüssel sowie die Anforderung nach bis zum Gültigkeitsende des neuen Zertifikats ausreichenden Schlüssellängen und zulässige Algorithmen betrachtet werden.

Zertifikate DÜRFEN NICHT erneuert werden, wenn diese gesperrt wurden.

Zertifikate DÜRFEN NICHT erneuert werden, wenn sich Angaben in den Zertifikaten geändert haben.

4.6.2 Antragsberechtigte für ein Renewal

Keine Vorgabe.

4.6.3 Verarbeitung von Anträgen auf Renewal

Wenn sich die Nutzungsbedingungen gegenüber den zur Zeit der Beantragung des Vorgängerzertifikats geltenden Nutzungsbedingungen geändert haben, MUSS die Akzeptanz dieser neuen Nutzungsbedingungen vor der Ausstellung eines neuen Zertifikats eingeholt werden.

Vor einer Erneuerung MÜSSEN die Gültigkeit des ablaufenden Zertifikats sowie der ursprünglichen vorgelegten Identifizierungsdaten und Attribute geprüft werden. Die Anträge MÜSSEN vollständig, korrekt, aktuell und autorisiert sein.

4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausstellung neuer Zertifikate

Siehe Kap. 4.3.2.

4.6.5 Verhalten, das die Annahme eines erneuerten Zertifikats bestätigt

Siehe Kap. 4.4.1.

4.6.6 Veröffentlichung erneuerter Zertifikate durch die TSP

Siehe Kap. 4.4.2.

4.6.7 Information Dritter über die Ausstellung neuer Zertifikate durch die TSP

Siehe Kap. 4.4.3.

4.7 Zertifikatserneuerung mit neuen Schlüsseln (Schlüsselerneuerung)

4.7.1 Umstände für eine Schlüsselerneuerung

Die Umstände und ggf. Zeiträume, unter denen eine Schlüsselerneuerung erlaubt ist, MÜSSEN in den CPS beschrieben werden.

Zertifikate DÜRFEN NICHT erneuert werden, wenn diese gesperrt wurden.

Zertifikate DÜRFEN NICHT erneuert werden, wenn sich Angaben in den Zertifikaten geändert haben.

4.7.2 Antragsberechtigte für eine Schlüsselerneuerung

Keine Vorgabe.

4.7.3 Verarbeitung von Anträgen auf Schlüsselerneuerung

Wenn sich die Nutzungsbedingungen gegenüber den zur Zeit der Beantragung des Vorgängerzertifikats geltenden Nutzungsbedingungen geändert haben, MUSS die Akzeptanz dieser neuen Nutzungsbedingungen vor der Ausstellung eines neuen Zertifikats eingeholt werden.

Vor einer Erneuerung MÜSSEN die Gültigkeit des ablaufenden Zertifikats sowie der ursprünglichen vorgelegten Identifizierungsdaten und Attribute geprüft werden. Die Anträge MÜSSEN vollständig, korrekt, aktuell und autorisiert sein.

[EVCP] In einem erneuerten Endteilnehmer-Zertifikat MÜSSEN das gleiche Ablaufdatum und der gleiche `subjectDN` wie im ursprünglichen Zertifikat gesetzt werden.

4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines erneuerten Zertifikats

Siehe Kap. 4.3.2.

4.7.5 Verhalten, das die Annahme eines erneuerten Zertifikats bestätigt

Siehe Kap. 4.4.1.

4.7.6 Veröffentlichung erneuerter Zertifikate durch die TSP

Siehe Kap. 4.4.2.

4.7.7 Information Dritter über die Ausstellung neuer Zertifikate durch den TSP

Siehe Kap. 4.4.3.

4.8 Änderung von Zertifikatsdaten

4.8.1 Umstände für eine Änderung von Zertifikatsdaten

Die Umstände und ggf. Zeiträume, unter denen eine Änderung von Zertifikatsdaten erlaubt oder erforderlich ist, MÜSSEN in den CPS beschrieben werden.

Wenn bei einer Änderung der Zertifikatsdaten der ursprüngliche Schlüssel wiederverwendet werden soll, MÜSSEN die Aspekte der Schwächung der Schlüssel sowie die Anforderung nach bis zum Gültigkeitsende des neuen Zertifikats ausreichenden Schlüssellängen und zulässige Algorithmen betrachtet werden.

Wenn ein Verdacht oder Nachweis über die Kompromittierung des ursprünglichen Schlüssels vorliegt oder das ursprüngliche Zertifikat aufgrund eines Sicherheitsvorfalls gesperrt wurde, DARF der ursprüngliche Schlüssel NICHT wiederverwendet werden.

Zertifikatsnehmer MÜSSEN verpflichtet werden, die Änderung von registrierten Daten im Gültigkeitszeitraum der auf Basis der registrierten Daten erstellten Zertifikate dem TSP zu melden. Zertifikatsnehmer MÜSSEN über die Prozesse zur Änderung der Zertifikatsdaten informiert werden.

4.8.2 Antragsberechtigte für eine Änderung von Zertifikatsdaten

Siehe Kap. 4.1.1.

4.8.3 Verarbeitung von Anträgen auf eine Änderung von Zertifikatsdaten

Wenn sich die Nutzungsbedingungen gegenüber den zur Zeit der Beantragung des Vorgängerzertifikats geltenden Nutzungsbedingungen geändert haben, MUSS die Akzeptanz dieser neuen Nutzungsbedingungen nachweislich vom Zertifikatsnehmer vor der Ausstellung eines neuen Zertifikats eingeholt werden.

Vor der Änderung von Zertifikatsdaten MUSS die Gültigkeit des ablaufenden Zertifikats sowie der nicht geänderten ursprünglich vorgelegten Identifizierungsdaten und Attribute des Subjekts geprüft werden, geänderte Daten MÜSSEN gemäß Kap. 3.2 validiert und registriert werden. Alle Daten MÜSSEN vollständig, korrekt, aktuell und autorisiert sein.

[3145] Die Generierung neuer Schlüssel MUSS erzwungen werden.

4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines erneuerten Zertifikats

Siehe Kap. 4.3.2.

4.8.5 Verhalten, das die Annahme eines geänderten Zertifikats bestätigt

Siehe Kap. 4.4.1.

4.8.6 Veröffentlichung geänderter Zertifikate durch die TSP

Siehe Kap. 4.4.2.

4.8.7 Information Dritter über die Ausstellung neuer Zertifikate durch den TSP

Siehe Kap. 4.4.3.

4.9 Zertifikatssperrung und Suspendierung

Die nachfolgend aufgeführten Anforderungen gelten nicht für „Kurzzeit-Zertifikate“, die durch die Erweiterung `id-etsi-ext-valassured-ST-certs` gekennzeichnet sind, wenn diese aufgrund ihrer kurzen Gültigkeit (kleiner als die Sperrfrist gemäß Kap. 4.9.5) grundsätzlich nicht gesperrt werden.

Wenn solche Kurzzeitzertifikate ausgestellt werden, MUSS in den CPS beschrieben werden, bei welchen Zertifikaten es sich um solche Kurzzeitzertifikate handelt und wie diese behandelt werden.

[TLS] [SMIME] Die nachfolgend aufgeführten Anforderungen gelten, sofern anwendbar, auch für Pre-Zertifikate.

4.9.1 Sperrgründe

Ergänzend zu den nachfolgend aufgeführten Sperrgründen DÜRFEN in den CPS weitere Sperrgründe festgelegt werden.

4.9.1.1 Gründe für die Sperrung eines Sub-CA Zertifikats

Ein Sub-CA-Zertifikat MUSS gesperrt werden, wenn

- ein schriftlicher Sperrantrag, auch ohne Angabe von Gründen, vom TSP gestellt wurde,
- festgestellt wird, dass der ursprüngliche Zertifikatsantrag nicht autorisiert war und auch nicht rückwirkend autorisiert werden kann oder soll,
- festgestellt wird, dass der private Schlüssel der Sub-CA kompromittiert oder einer nicht autorisierten Person oder Organisation bekannt gegeben wurde, oder nicht mehr den Anforderungen (siehe Kap. 6.1.5 und 6.1.6) entspricht,
- festgestellt wird, dass das Zertifikat missbräuchlich eingesetzt wurde,
- festgestellt wird, dass das Sub-CA-Zertifikat nicht konform zu dieser CP herausgegeben wurde oder der Betreiber der Sub-CA nicht konform zu dieser CP arbeitet,
- festgestellt wird, dass Information im Zertifikat nicht korrekt oder missverständlich sind,
- der Betrieb der Root-CA oder der Sub-CA eingestellt wird und keine Regelungen zur Weiterführung des Sperr-Service getroffen wurden,
- das Recht des Betreibers der Root-CA oder Sub-CA, Zertifikate gemäß den Anforderungen dieser CP auszustellen, erlischt oder widerrufen oder beendet wird und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen wurden.

Bei Sperrung eines CA-Zertifikats MUSS der am besten passende Sperrgrund gemäß [RFC5280] gesetzt werden.

4.9.1.2 Gründe für die Sperrung eines Endteilnehmer-Zertifikats

Ein Zertifikat MUSS gesperrt werden, wenn

- ein autorisierter Sperrantrag, auch ohne Angabe von Gründen, vom Zertifikatsnehmer oder, sofern anwendbar, der zuständigen RA vorliegt,
- relevante Angaben im Zertifikat nicht (mehr) korrekt sind,
  Anm.: erlaubte Abweichungen MÜSSEN in den CPS beschrieben werden.
- keine Autorisierung des Zertifikats (mehr) vorliegt, dazu zählen:
  - Eine Information vom Zertifikatsnehmer liegt vor, dass der ursprüngliche Zertifikatsantrag nicht autorisiert war und auch nicht rückwirkend autorisiert werden kann oder soll.
  - [TLS] Es kann der Kontrolle über einen/eine im Zertifikat angegebenen FQDN oder IP-Adresse nicht mehr vertraut werden.
  - [TLS] Die Verwendung eines im Zertifikat angegebenen FQDN oder einer IP-Adresse ist nicht mehr zulässig.
  - [SMIME] Es kann der Domain-Autorisierung oder der Kontrolle über die Mailbox nicht mehr vertraut werden
  - [SMIME] Die Verwendung einer im Zertifikat angegebenen E-Mail-Adresse bzw. FQDN ist nicht mehr zulässig.

- eine Schlüsselschwäche oder -kompromittierung nachgewiesen wird, dazu zählt, dass der private Schlüssel
  - einer unautorisierten Person übergeben wurde,
  - leicht auf Basis des öffentlichen Schlüssels berechnet werden (z.B. „Debian weak key“) kann,
  - unter Verwendung einer mangelhaften Methode generiert wurde oder durch bekannte Methoden gefährdet ist,
  - nicht mehr den Anforderungen gemäß Kap. 6.1.5 und 6.1.6 genügt,
- ein Verstoß gegen die CP, CPS oder die Nutzungsbedingungen nachgewiesen wird, dazu zählen:
  - Das Zertifikat wurde nicht in Übereinstimmung mit dem relevanten CPS ausgestellt.
  - Das Zertifikat wurde missbräuchlich eingesetzt.
  - [TLS] Ein Wildcard-Zertifikat wurde zur Authentifizierung eines betrügerisch irreführenden Sub-FQDN verwendet.
  - Der Zertifikatsnehmer wurde, sofern anwendbar, suspendiert bzw. gesperrt.

Darüber hinaus MÜSSEN alle betroffenen Zertifikate gesperrt werden, wenn

- der TSP seinen Betrieb einstellt und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen hat,
- der TSP die Berechtigung verliert, bestimmte Zertifikatstypen auszustellen und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen hat,
- der private Schlüssel einer CA kompromittiert wurde oder
- [QCP-l-qscd] [QCP-n-qscd] die Zertifizierung der verwendeten QSCD ausläuft oder die QCSD nicht akzeptable Sicherheitsmängel aufweisen.

Bei Sperrung eines Endteilnehmern-Zertifikats MUSS, sofern die Angabe eines Sperrgrundes gefordert ist, der korrekte Sperrgrund wie folgt ausgewählt werden:

- `keyCompromise` (Schlüsselkompromittierung) MUSS gewählt werden, wenn der private Schlüssel des Zertifikatsnehmers kompromittiert wurde.
  [TLS] [SMIME] `keyCompromise` MUSS auch dann ausgewählt werden, wenn der TSP erfährt, dass der private Schlüssel potenziell kompromittiert werden kann, z.B. weil dieser leicht auf Basis des öffentlichen Schlüssels berechnet werden kann (z.B. Debian Weak Key) oder die Methode zur Generierung des privaten Schlüssels fehlerhaft war oder eine Methode existiert, die den privaten Schlüssel des Zertifikatsnehmers enthüllen könnte.
- `cessationOfOperation` (Beendigung der Zertifikatsnutzung) MUSS gewählt werden, wenn der Zertifikatsnehmer die Nutzung des Zertifikats beendet.
  [TLS] [SMIME] `cessationOfOperation` MUSS auch dann gewählt werden, wenn der Zertifikatsnehmer keine Kontrolle mehr über die im Zertifikat angegebenen Domain Namen, IP-Adressen oder E-Mail-Adressen hat oder nicht mehr autorisiert ist, diese zu verwenden.
- `affiliationChanged` (Zugehörigkeit geändert) MUSS gewählt werden, wenn sich Attribute im `subjectDN` oder andere Daten im Zertifikat geändert haben.
- `superseded` (abgelöst) MUSS gewählt werden, wenn das Zertifikat durch ein Folgezertifikat ersetzt und nicht länger benötigt wird.
  [TLS] [SMIME] `superseded` MUSS auch dann gewählt werden, wenn die CA erfährt, dass der Domainvalidierung nicht vertraut werden kann, dass das Zertifikat nicht gemäß dem relevanten CPS erstellt wurde oder das Zertifikat nicht mehr den Anforderungen nach Kap. 6.1.5 und 6.1.6 genügt.

- `privilegeWithdrawn` (Recht entzogen) MUSS gewählt werden, wenn dem Zertifikatsnehmer das Recht zur Nutzung des Zertifikats entzogen wird, weil z.B. der Zertifikatsantrag nicht autorisiert war, das Zertifikat missbräuchlich verwendet wurde oder der Zertifikatsnehmer gegen Verpflichtungen verstoßen hat.
  [TLS] [SMIME] `privilegeWithdrawn` MUSS auch dann gewählt werden, wenn ein Wildcard-Zertifikat verwendet wurde, um einen betrügerisch irreführenden untergeordneten voll qualifizierten Domänennamen zu authentifizieren oder sich die Informationen im Zertifikat wesentlich geändert haben oder nicht korrekt sind.
  HINWEIS: `privilegeWithdrawn` DARF in der Liste der von den Zertifikatsnehmern auswählbaren Sperrgründe weggelassen werden, da dieser Sperrgrund durch den TSP gesetzt wird.

In allen anderen Fällen SOLLTE `unspecified` (unspezifiziert) als Sperrgrund gewählt werden.

[TLS] In allen anderen Fällen MUSS `unspecified` als Sperrgrund gewählt werden.

4.9.2 Berechtigte Sperrantragsteller

Die Sperrung einer Sub-CA MUSS grundsätzlich durch einen berechtigten Vertreter des TSP beantragt werden. Sollte einer der in Kap. 4.9.1.1 aufgeführten Sperrgründe von der Telekom Security als Betreiber der Root-CAs festgestellt werden, so DARF die Sperrung durch die Telekom Security auch ohne vorliegenden Sperrantrag durchgeführt werden.

[3145] Die Sperrung einer Sub-CA im Anwendungsbereich der TR-03145 liegt nicht im Geltungsbereich dieser CP, da die Sub-CA-Zertifikate nicht von einer Root-CA der Telekom ausgestellt werden. Die Sperrung der Sub-CAs MUSS gemäß den Vorgaben des zuständigen Root-CA-Betreibers erfolgen.

Die Sperrung eines Endteilnehmer-Zertifikats MUSS grundsätzlich durch den Zertifikatsnehmer selbst oder die zuständige RA beantragt werden. Sollte einer der in Kap. 4.9.1.2 aufgeführten Sperrgründe festgestellt oder durch einen Dritten gemeldet und vom TSP nachvollzogen werden können, so MUSS eine Sperrung durch den TSP veranlasst werden.

[QCP-n] [QCP-l] Wenn ein Zertifikat Angaben über eine Vertretungsmacht Dritter oder amts- und berufsbezogene oder sonstige Angaben gemäß [VDG§12] enthält, so DARF auch die vertretene Person oder Organisation oder die für die amts- und berufsbezogenen oder sonstigen Angaben zur Person zuständige Organisation eine Sperrung verlangen, wenn

- die Vertretungsmacht oder
- die Voraussetzungen für die amts- und berufsbezogenen oder sonstigen Angaben zur Person nach Aufnahme in das qualifizierte Zertifikat

entfallen.

[VS-NfD] Ein Endteilnehmer-Zertifikat MUSS auch auf ein begründetes Verlangen des Sicherheitsbeauftragten gesperrt werden.

4.9.3 Ablauf einer Sperrung

Zur Sperrung von Zertifikaten aller Hierarchieebenen MÜSSEN ständig verfügbare Schnittstellen (7x24h) zur Übergabe von Sperranträgen oder Problemmeldungen, die zur Sperrung von Zertifikaten führen können, sowie Anleitungen zur Nutzung dieser Schnittstellen bereitgestellt werden.

Sperrungen DÜRFEN NICHT durchgeführt werden, wenn diese nicht von berechtigten Sperrantragstellern beantragt wurden oder auf Problemmeldungen beruhen, die nicht als berechtigter Auslöser einer Sperrung eingestuft wurden.

Der Zertifikatsnehmer und, sofern davon abweichend, der Sperrantragsteller, MÜSSEN sofern möglich über durchgeführte Sperrungen informiert werden.

Endgültig gesperrte Zertifikate DÜRFEN NICHT wieder entsperrt werden.

[VS-Nfd] Die Abläufe zur Sperrung von Endteilnehmer-Zertifikaten inkl. der festgelegten Fristen MÜSSEN vom Sicherheitsbeauftragten freigegeben werden.

4.9.4 Fristen zur Beantragung einer Sperrung

Sobald ein Sperrgrund gemäß Kap. 4.9.1 festgestellt wird, MUSS unverzüglich ein Sperrantrag gestellt werden.

4.9.5 Fristen zur Verarbeitung von Sperranträgen durch die TSP

Ergänzend zu den nachfolgend aufgeführten Fristen DÜRFEN in den CPS kürzere Fristen für bestimmte Sperrgründe festgelegt werden.

Sub-CA-Zertifikate MÜSSEN in Abhängigkeit der Umstände innerhalb einer angemessenen Frist gesperrt werden.

[TLS] [SMIME] Sub-CA-Zertifikate MÜSSEN innerhalb von sieben Tagen nach Erhalt eines autorisierten Sperrantrags gesperrt werden. Diese Frist beinhaltet die Zeit zur Umsetzung des Sperrstatus in den Zertifikatsstatusdiensten.

Nach der Sperrung eines Sub-CA-Zertifikats MUSS der entsprechende Eintrag in der CCADB aktualisiert werden. Wenn die Sperrung des Sub-CA-Zertifikats aufgrund eines Sicherheitsvorfalls erforderlich ist, MUSS die CCADB innerhalb von 24 Stunden upgedatet werden, ansonsten innerhalb von 7 Tagen.

Endteilnehmer-Zertifikate MÜSSEN grundsätzlich so schnell wie möglich, jedoch spätestens innerhalb von 24 Stunden nach Eingang eines autorisierten Sperrantrags gesperrt werden. Diese Frist beinhaltet die Zeit zur Umsetzung des Sperrstatus in den Zertifikatsstatusdiensten.

Davon ausgenommen sind Sperrungen, die für einen späteren Zeitpunkt beantragt werden, z.B. aufgrund einer geplanten Beendigung der Teilnahme. In diesem Fall DARF, sofern dieses Vorgehen im CPS beschrieben ist, das im Sperrantrag aufgeführte Wunschdatum zur Sperrung des Zertifikats als Eingangsdatum des autorisierten Sperrantrags gesetzt werden.

Für Sperrungen, die nicht auf autorisierten Sperranträgen, sondern auf anderen der in Kap. 4.9.1.2 aufgeführten Sperrgründe basieren, MÜSSEN in den CPS die Sperrfristen festgelegt werden.

[TLS] [SMIME] Abweichend von der grundsätzlich festgelegten Sperrfrist von 24 Stunden gelten folgende Ausnahmen: Zertifikate SOLLTEN innerhalb von 24 Stunden und MÜSSEN innerhalb von 5 Tagen gesperrt werden, wenn

- die Methode zur Generierung des privaten Schlüssels fehlerhaft war oder eine Methode existiert, die den privaten Schlüssel des Zertifikatsnehmers enthüllen könnte,
- der Zertifikatsnehmer nicht mehr autorisiert ist, die im Zertifikat angegebenen Domain Namen, IP-Adressen oder E-Mail-Adressen zu verwenden oder sich die Informationen im Zertifikat wesentlich geändert haben oder nicht korrekt sind,
- das Zertifikat nicht gemäß dem relevanten CPS erstellt wurde oder nicht mehr den aktuellen Anforderungen nach Kap. 6.1.5 und 6.1.6 genügt,
- das Zertifikat missbräuchlich verwendet wurde oder der Zertifikatsnehmer gegen Verpflichtungen verstoßen hat oder
- der TSP das Recht verliert, Zertifikate nach [BR] bzw. [SBR] auszustellen.

Die TSP MÜSSEN jedoch auch in der Lage sein, in begründeten Fällen Zertifikate zu einem von einem Root-Store-Betreiber vorgegebenen Termin zu sperren, der von den o.g. Fristen abweicht.

Die TSP MÜSSEN rund um die Uhr in der Lage sein, auf hochpriorisierte Problemmeldungen zu reagieren und bei Bedarf eine Meldung an Strafverfolgungsbehörden weiterzuleiten und / oder die von dem Problem betroffenen Zertifikate zu sperren.

Innerhalb von 24 Stunden nach Eingang einer Problemmeldung MÜSSEN die Fakten und Umstände untersucht werden und es MUSS dem Zertifikatsnehmer sowie der meldenden Person eine erste Rückmeldung zu den bis dahin vorliegenden Erkenntnissen gegeben werden. Anschließend MÜSSEN mit dem Zertifikatsnehmer und der meldenden Person die Analyseergebnisse besprochen werden und es MUSS entschieden werden, ob eine Sperrung erforderlich ist.

Falls eine Sperrung aufgrund einer Problemmeldung erforderlich ist, MUSS unter Beachtung der o.g. zeitlichen Vorgaben und Berücksichtigung der folgenden Aspekte der Zeitpunkt der Sperrung festgelegt werden:

- die Art des mutmaßlichen Problems (Umfang, Kontext, Schweregrad, Ausmaß, Schadensrisiko)
- die Auswirkungen einer Sperrung (direkte und kollaterale Auswirkungen auf Zertifikatsnehmer und Zertifikatsnutzer)
- die Anzahl der Problemmeldungen zu einem Zertifikat oder Zertifikatsnehmer
- die Entität, welche die Meldung eingestellt hat
- die einschlägigen Rechtsvorschriften

4.9.6 Anforderungen an Zertifikatsnutzer zur Prüfung von Sperrinformationen

Zertifikatsnutzer SOLLTEN zur Prüfung des Status von Zertifikaten die Zertifikatsstatusdienste gemäß Kap. 4.10 abfragen.

Zertifikatsnutzer DÜRFEN bei Kurzzeitzertifikaten darauf verzichten, den Status abzufragen.

4.9.7 Frequenz der Veröffentlichung von Sperrlisten

Certification Authority Revocation Lists (CARLs) MÜSSEN innerhalb von 24 Stunden nach Sperrung eines Sub-CA-Zertifikats sowie regelmäßig mindestens alle 12 Monate aktualisiert werden.

Certificate Revocation Lists (CRLs) MÜSSEN regelmäßig mindestens alle 24 Stunden aktualisiert werden.

[3145] CRLs MÜSSEN ergänzend zur regelmäßigen Ausstellung auch im Anschluss an die Sperrung eines Endteilnehmer-Zertifikats aktualisiert und veröffentlicht werden.

4.9.8 Maximale Latenzzeit von Sperrlisten

Keine Vorgabe.

4.9.9 Verfügbarkeit von Online-Sperr-/Statusinformationen

Siehe Kap. 4.10.

4.9.10 Anforderungen an Online-Überprüfungsverfahren

Zertifikatsnutzer sollten bei der Prüfung des Zertifikatsstatus per OCSP die Vorgaben zur Verarbeitung von OCSP-Antworten gemäß [RFC6960] berücksichtigen.

4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Keine Vorgabe.

4.9.12 Gesonderte Bedingungen bei Kompromittierung privater Schlüssel

Keine Vorgabe.

[TLS] [SMIME] Die akzeptierten Methoden zum Nachweis einer Schlüsselkompromittierung MÜSSEN in den CPS in Kap. 4.9.12 beschrieben werden.

Bzgl. der Meldung einer vermuteten Schlüsselkompromittierung siehe Kap. 1.5.2.

4.9.13 Umstände für eine Suspendierung

Sofern eine Suspendierung erlaubt ist und angeboten wird, MÜSSEN die Umstände für eine Suspendierung im CPS beschrieben werden.

Sub-CA Zertifikate DÜRFEN NICHT suspendiert werden.

[TLS] [SMIME-Strict] Endteilnehmer-Zertifikate DÜRFEN NICHT suspendiert werden.

[3145] Ergänzend zur Sperrung oder Suspendierung von Zertifikaten MÜSSEN Zertifikatsnehmer suspendiert werden, wenn festgestellt wird, dass diese ihre Pflichten nicht mehr erfüllen, z.B. bei einem Zertifikatsmissbrauch.

4.9.14 Berechtigte Antragsteller für eine Suspendierung

Keine Vorgabe.

4.9.15 Ablauf einer Suspendierung

Keine Vorgabe.

4.9.16 Begrenzung der Suspendierungsperiode

Keine Vorgabe.

4.10 Zertifikatsstatusdienste

Mindestens über die Gültigkeitsdauer aller ausgestellten Sub-CA und Endteilnehmer-Zertifikate MÜSSEN authentische und integre Zertifikatsstatusdienste in Form von Sperrlisten und/oder OCSP-Auskünften bereitgestellt werden.

Zu den Endteilnehmer-Zertifikaten SOLLTEN OCSP-Auskünfte bereitgestellt werden.

[TLS] [SMIME] Zu Sub-CA und Endteilnehmer-Zertifikaten MÜSSEN Sperrlisten und OCSP-Auskünfte bereitgestellt werden. Dies gilt auch für Pre-Zertifikate.

[QEVCP-w] Die Zertifikatsstatusdienste MÜSSEN über die Zertifikatsgültigkeit hinaus bereitgestellt werden, die Bereitstellungszeit MUSS im CPS beschrieben werden. Die Integrität der Statusinformationen MUSS über die gesamte Bereitstellungszeit gewährleistet werden.

[QCP-n] [QCP-l] Die Zertifikatsstatusdienste MÜSSEN über die gesamte Zeit des Betriebs des Trust Services angeboten werden. Die Integrität der Statusinformationen MUSS über die gesamte Bereitstellungszeit gewährleistet werden.

4.10.1 Betriebliche Vorgaben

Zertifikatsstatusdienste MÜSSEN mindestens alle 24 Stunden zeitsynchronisiert (UTC) werden.

Wenn Sperrlisten und OCSP-Auskünfte bereitgestellt werden, MÜSSEN diese unter Berücksichtigung der unterschiedlichen Aktualisierungsfristen beider Methoden spätestens nach 24 Stunden konsistent sein. Ggf. voneinander abweichende Aktualisierungsfristen MÜSSEN in den CPS aufgeführt werden und es MUSS beschrieben werden, wie daraus resultierende unterschiedliche Prüfergebnisse zu interpretieren sind.

4.10.1.1 Betriebliche Vorgaben für die Bereitstellung der OCSP-Responder

OCSP-Responder MÜSSEN konform zum [RFC6960] betrieben werden. Konkretisierend zum [RFC6960] gilt, dass Anfragen zu Zertifikaten mit nicht bekannten Zertifikatseriennummern NICHT mit dem Status `good` beantwortet werden DÜRFEN.

Die zu wählende Antwort hängt von der Arbeitsweise des OCSP-Responders ab:

- Bei vorproduzierten OCSP-Antworten MÜSSEN solche Anfragen mit der Fehlermeldung `unauthorized` beantwortet werden.
- Bei ad hoc erzeugten OCSP-Antworten SOLLTEN solche Anfragen mit dem Status `unknown` beantwortet werden.
  Es DÜRFEN bei adhoc erzeugten OCSP-Antworten solche Anfragen auch mit dem Status `revoked` beantwortet werden, dann MUSS jedoch die Erweiterung `id-pkix-ocsp-extended-revoke` gemäß [RFC6960#4.4.8] gesetzt werden.

OCSP-Anfragen zu nicht vergebenen Seriennummern SOLLTEN protokolliert werden.

OCSP-Antworten DÜRFEN vorgehalten und innerhalb ihrer Gültigkeit[5] für weitere Anfragen wiederverwendet werden.

[TLS] [SMIME] OCSP-Antworten zu Sub-CA-Zertifikaten DÜRFEN eine Gültigkeit von maximal 12 Monaten NICHT überschreiten. Nach einer Sperrung eines Sub-CA-Zertifikats MUSS innerhalb von 24 Stunden eine aktualisierte Auskunft im OCSP-Responder abrufbar sein.

OCSP-Antworten zu Endteilnehmer-Zertifikaten MÜSSEN eine Gültigkeit von mindestens 8 Stunden jedoch maximal 7 Tagen haben. Sie DÜRFEN jedoch NICHT die Gültigkeitsdauer, des ausstellenden Sub-CA-Zertifikats oder des in der OCSP-Antwort im Feld `certs` enthaltenen Zertifikats überschreiten.

Für die Aktualisierung von OCSP-Antworten gelten folgende Bedingungen:

- Falls die OCSP-Antworten eine Gültigkeit von weniger als 16 Stunden haben, MÜSSEN diese nach Ablauf der Hälfte ihrer Gültigkeit aktualisiert werden.
- Falls die OCSP-Antworten eine Gültigkeit von 16 Stunden oder mehr haben, MÜSSEN diese spätestens 4 Tage nach ihrer Ausstellung und nicht später als 8 Stunden vor Ablauf Ihrer Gültigkeit aktualisiert werden.

[QCP-n] [QCP-l] Ein Gültigkeitsende DARF gesetzt werden.

[5] „Gültigkeit“ bezieht sich in diesem Kontext auf die Angabe eines Datums im Attribut `nextUpdate`, d.h. dem Zeitpunkt, zu dem spätestens eine neue Statusinformation per OCSP abgerufen werden kann

4.10.1.2 Betriebliche Vorgaben für die Bereitstellung der Sperrlisten

Alle Sperrlisten MÜSSEN über den Zeitpunkt der nächsten regelmäßigen Aktualisierung hinaus gültig[6] sein.

Die Gültigkeitsdauer einer letzten Sperrliste zu den Zertifikaten ihres Anwendungsbereichs SOLLTE auf den Wert `99991231235959Z` gesetzt werden.

Gesperrte Zertifikate DÜRFEN grundsätzlich nach ihrem Gültigkeitsende aus der Sperrliste entfernt werden, sie MÜSSEN jedoch noch in der nächsten regulären Sperrliste nach ihrem Gültigkeitsende enthalten sein.

[TLS] [SMIME] CARLs DÜRFEN eine Gültigkeit von 12 Monaten NICHT überschreiten, CRLs DÜRFEN eine Gültigkeit von 10 Tagen NICHT überschreiten.

[QCP] Wenn Sperrlisten und OCSP-Auskünfte bereitgestellt werden, SOLLTEN abgelaufene Zertifikate NICHT aus der Sperrliste entfernt werden. Wenn ausschließlich Sperrlisten angeboten werden, DÜRFEN abgelaufene Zertifikate NICHT aus der Sperrliste entfernt werden. Wenn Sperrlisten bereitgestellt werden, DARF eine letzte Sperrliste NICHT ausgestellt werden, bevor alle Zertifikate in ihrem Anwendungsbereich abgelaufen oder gesperrt sind.

4.10.2 Verfügbarkeit

Die Zertifikatsstatusdienste MÜSSEN 7x24h zur Verfügung zu stehen. Im Falle von Störungen MÜSSEN größtmögliche Bemühungen unternommen werden, die Störungen innerhalb der festgelegten Entstörungsfristen zu beheben.

[TLS] [SMIME] Es MÜSSEN ausreichende Kapazitäten zur Verfügung gestellt werden, so dass die Antwortzeit unter normalen Betriebsbedingungen 10 Sekunden nicht überschreitet.

[3145] [NCP] Die maximale Ausfallzeit der Systeme MUSS in den CPS aufgeführt werden.

4.10.3 Optionale Merkmale

Keine Vorgabe.

4.11 Kündigung durch den Zertifikatsnehmer

Keine Vorgabe.

[6] „Gültigkeit“ bezieht sich in diesem Kontext auf die Angabe eines Datums im Attribut `nextUpdate`, d.h. dem Zeitpunkt, zu dem spätestens eine neue Sperrliste abgerufen werden kann

4.12 Schlüsselhinterlegung und Wiederherstellung

4.12.1 Schlüsselhinterlegungs- und Wiederherstellungsrichtlinien und -Praktiken

Wenn ein TSP Schlüsselhinterlegung anbietet, so

- DÜRFEN Verschlüsselungsschlüssel hinterlegt werden,
- DÜRFEN Authentisierungsschlüssel und Signaturschlüssel NICHT in einer Form hinterlegt werden, die ein Entschlüsseln dieser Schlüssel ohne Kontrolle des Zertifikatsnehmers ermöglichen,
- MUSS sichergestellt werden, dass alle Kopien der privaten Schlüssel unter dem gleichen Sicherheitslevel aufbewahrt werden, wie das Original und nur an autorisierte Empfänger herausgegeben werden,
- DÜRFEN NICHT mehr Kopien der privaten Schlüssel erzeugt werden, wie für die Sicherstellung der Kontinuität erforderlich sind,
- DARF ein privater Schlüssel, den der TSP oder eine festgelegte Rolle zur Entschlüsselung der hinterlegten Schlüssel nutzt, NICHT zu anderen Zwecken genutzt werden.

4.12.2 Richtlinien und Praktiken zur Kapselung und Wiederherstellung von Sitzungsschlüsseln

Keine Vorgabe.

5 BAULICHE, ORGANISATORISCHE UND BETRIEBLICHE REGELUNGEN

In einer vom Management freigegebenen Informationssicherheitsrichtlinie MUSS der Ansatz zum Management der Informationssicherheit festgelegt werden und es MUSS ein geeignetes Informationssicherheits-Management-System (ISMS, z.B. in Anlehnung an ISO 27001) etabliert werden, welches unter anderem

- die Entwicklung, Einführung und Aufrechterhaltung der Sicherheitskonzepte inkl. regelmäßiger Risikoanalysen zu den Trust Services verwaltet,
- die Informationen inventarisiert und gemäß dem Risikomanagement klassifiziert,
- in das Changemanagement zu sicherheitskritischen Änderungen involviert ist und
- eine regelmäßige Auditierung der Trust Services inkl. deren Dokumentation vorsieht.

Die Informationssicherheitsrichtlinie MUSS regelmäßig sowie bei Bedarf revidiert und an alle Mitarbeiter kommuniziert werden.

Die Sicherheitskonzepte MÜSSEN die folgenden Anforderungen erfüllen:

- Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Zertifikatsdaten und des Zertifikatsmanagements-Prozesses.
- Schutz gegen mögliche Bedrohungen und Gefahren für die Vertraulichkeit, Integrität und Verfügbarkeit der Zertifikatsdaten und des Zertifikatsmanagement-Prozesses.
- Schutz gegen unautorisierten oder ungerechtfertigten Zugriff, Nutzung, Veröffentlichung, Auswechselung oder Zerstörung von Zertifikatsdaten oder des Zertifikatsmanagement-Prozesses.
- Schutz gegen Verlust oder mutwillige Zerstörung von Zertifikatsdaten oder Manipulationen im Zertifikatsmanagement-Prozess.
- Einhaltung von gesetzlich geforderten Sicherheitsanforderungen.

Die Sicherheitskonzepte MÜSSEN insbesondere folgende Aspekte berücksichtigen:

- Physikalische Sicherheit (Gebäude und Umfeld),
- Integritätssicherung der Systeme (inkl. Konfigurationsmanagement) sowie der verwendeten vertrauenswürdigem Codes,
- Malware-Erkennung und Verhinderung,
- Netzwerksicherheit und Firewall Management,
- Benutzer- und Rollenmanagement inkl. der Prozesse zur Vergabe vertrauenswürdiger Rollen
- Schulung, Sensibilisierung und Fortbildung der Mitarbeiter,
- Logische Zugriffskontrolle,
- Protokollierung und
- automatische Sperrung der Arbeitsplätze bei Inaktivität.

Risikoanalysen, welche die vorhersehbaren internen und externen Bedrohungen, die zu einem unautorisierten Zugriff, Veröffentlichung, Missbrauch, Austausch oder Zerstörung von Zertifikatsdaten oder des Zertifikatsmanagement-Prozesses führen können, identifizieren, analysieren und bewerten, MÜSSEN jährlich durchgeführt werden.

Die Risikoanalysen MÜSSEN die Wahrscheinlichkeiten und die potenziellen Schäden dieser Bedrohungen unter Berücksichtigung der Sensibilität der Zertifikatsdaten und des Zertifikatsmanagement-Prozesses betrachten und die Angemessenheit der Richtlinien, Verfahren, Informationssysteme, Technologien und weiterer Vorkehrungen bewerten, die getroffen wurden, um den Bedrohungen entgegenzuwirken.

Auf Basis der Bewertung der Risiken MÜSSEN geeignete, angemessene Risikobehandlungsmaßnahmen (z.B. bauliche, organisatorische, personelle sowie dem Stand der Technik entsprechende technische Sicherheitsmaßnahmen) entwickelt und deren Umsetzung im ISMS gemanagt und kontrolliert werden.

Die Risikobewertung sowie ggf. identifizierte Restrisiken müssen vom Management der TSP genehmigt werden.

[VS-NfD] Bevor IT-Systeme für VS-NfD eingesetzt werden, MÜSSEN diese bzgl. der Einhaltung der erforderlichen Geheimschutzmaßnahmen gemäß [VSA] überprüft werden.

5.1 Physikalische Maßnahmen

Zur Vermeidung von Verlust, Diebstahl, Schaden oder Kompromittierung von Anlagen, Medien und Informationen MÜSSEN physikalische Maßnahmen getroffen werden.

5.1.1 Standort und Bauweise

Die Systeme MÜSSEN an geeigneten Standorten in sicheren Räumlichkeiten mit hinreichendem physikalischem Schutz betrieben werden, bei der Wahl der Standorte MÜSSEN mögliche Naturkatastrophen (z.B. Hochwasser) sowie die Wiederherstellung nach Katastrophen berücksichtigt werden.

Wenn Räumlichkeiten mit anderen Organisationen geteilt werden, die nicht zum TSP gehören, MÜSSEN die nicht zum TSP gehörenden Systeme außerhalb des Bereichs betrieben werden, in dem die CA- und Statusdienst-Systeme des TSP betrieben werden. Die verschiedenen Bereiche MÜSSEN durch geeignete physikalische Barrieren voneinander getrennt sein.

Die Systeme der TSP DÜRFEN gemäß der sich aus der Risikobewertung ergebenden Kritikalität oder den an sie gestellten Sicherheitsanforderungen in unterschiedlichen Sicherheitszonen betrieben werden, wobei insbesondere die Systeme der Root-CA getrennt vom normalen Betrieb in einer hochsicheren Zone betrieben werden MÜSSEN.

[VS-NfD] Die Hinweise für den Schutz von VSIT-Räumen nach § 29 VSA [VSIT] MÜSSEN als Anleitung berücksichtigt werden.

5.1.2 Physikalischer Zutritt

Der Zugang zu den Räumlichkeiten, in denen die Systeme der TSP betrieben werden, MUSS über geeignete Zugangskontrollen auf die zutrittsberechtigten Personen in vertrauenswürdigen Rollen beschränkt werden. Sofern nicht-autorisierte Personen Zutritt zu diesen Räumlichkeiten benötigen, MÜSSEN diese immer durch eine autorisierte Person begleitet werden.

Die Räumlichkeiten, in denen die Systeme der TSP betrieben werden, MÜSSEN über eine Alarmierung zur Erkennung von unautorisierten Zutritten verfügen.

Die erteilten Zutrittsberechtigungen MÜSSEN regelmäßig überprüft werden.

5.1.3 Stromversorgung und Klimatisierung

Eine unterbrechungsfreie Stromversorgung sowie Klimatisierung der Systeme entsprechend der sich aus der Risikobewertung ergebenden Kritikalität sowie der vereinbarten Service-Level MUSS gewährleistet sein.

5.1.4 Wassereinwirkung

Die Räume in denen Komponenten des TSP betrieben werden, MÜSSEN entsprechend der sich aus der Risikobewertung ergebenden Kritikalität vor Wassereinwirkung geschützt werden.

5.1.5 Brandvorsorge und Brandschutz

Die Räume in denen Komponenten des TSP betrieben werden, MÜSSEN entsprechend der sich aus der Risikobewertung ergebenden Kritikalität vor Zerstörung durch Feuer geschützt werden.

5.1.6 Aufbewahrung von Medien

Maßnahmen zum Schutz vor unbeabsichtigter Verwendung außerhalb der gesicherten Umgebung, Beschädigung, Diebstahl, unbefugtem Zugriff und Veralterung der relevanten Medien der TSP MÜSSEN getroffen werden. Bei diesen Maßnahmen MUSS die Aufbewahrungsfrist der Medien berücksichtigt werden. Alle Medien MÜSSEN entsprechend der Klassifizierung der darauf gespeicherten Informationen sicher behandelt werden.

5.1.7 Abfallentsorgung

Zur Verhinderung der unbefugten Nutzung oder des unbefugten Zugriffs auf Informationen MÜSSEN sichere Entsorgungsprozesse etabliert werden. Insbesondere Medien, die sensible Daten enthalten, MÜSSEN sicher entsorgt werden, wenn sie nicht mehr benötigt werden.

5.1.8 Externe Sicherung

Keine Vorgabe.

5.2 Organisatorische Maßnahmen

5.2.1 Vertrauenswürdige Rollen

Zur Gewährleistung eines sicheren Betriebs MÜSSEN die TSP über eine geeignete Organisation verfügen, in der mindestens die folgenden vertrauenswürdigen Rollen abgebildet sind:

- Leiter Trust Center: trägt die gesamte Verantwortung für die Dienste des TSP
- Leiter VDA: ist Ansprechpartner und Auskunftsperson für die nationalen Aufsichtsbehörden für die qualifizierten Vertrauensdienste
- Solution Manager: verantwortet und verwaltet einen Trust Service
- Trust Center Information Security Officer: hat die übergreifende Verantwortung für die Implementierung von Sicherheitsmaßnahmen
- Registrierungsmitarbeiter/Validierungsspezialist: prüft und bearbeitet Anträge zur Zertifikatsausstellung, -suspendierung, -sperrung oder -erneuerung
- Administrator: installiert, konfiguriert und wartet die Systeme der Trust Services
- interner Auditor: prüft regelmäßig sowie bei Unstimmigkeiten z.B. Protokolldaten, Datenbanken und papierbasierte Dokumentationen der Trust Services
- Compliance-Manager: prüft regelmäßig die den Trust Services zugrunde liegenden Anforderungen, stimmt diese mit den Solution Managern ab und koordiniert die erforderlichen Prüfungen durch externe Auditoren.

Die relevanten Rollen incl. einer Übersicht der zugewiesenen Tätigkeiten MÜSSEN im CPS beschrieben werden.

5.2.2 Anzahl der für eine Aufgabe erforderlichen Personen

Für alle in Kap. 5.2.1 aufgeführten Rollen MUSS mindestens ein Vertreter benannt werden.

Sicherheitsrelevante oder -kritische Tätigkeiten, wie z.B. Generierung, Sicherung und Wiederherstellung von CA-Schlüsseln, MÜSSEN im Vier-Augen-Prinzip durch Personen in vertrauenswürdigen Rollen durchgeführt werden. Die Anzahl der Mitarbeiter, die solche sicherheitsrelevanten oder -kritischen Tätigkeiten ausüben, MUSS auf ein Minimum beschränkt sein.

Die sicherheitsrelevanten und -kritischen Tätigkeiten, für die ein Vier-Augen-Prinzip (oder mehr) benötigt wird, MÜSSEN im CPS beschrieben werden.

[EVCP] Zertifikatsanträge MÜSSEN im Vier-Augen-Prinzip validiert und freigegeben werden, siehe Kap. 4.2.1. Zur Sicherstellung des Vier-Augen-Prinzips MÜSSEN auditierbare Sicherheitsmaßnahmen umgesetzt werden.

5.2.3 Identifizierung und Authentifizierung für vertrauenswürdige Rollen

Die Identifizierung geeigneter Personen zur Besetzung von Rollen, die Übertragung der Rollen sowie deren Entzug MÜSSEN nach einem dokumentierten Prozess erfolgen.

Die Rolleninhaber MÜSSEN vom Management des TSP offiziell in die vertrauenswürdige Rolle berufen werden.

Vor der Übertragung einer vertrauenswürdigen Rolle MUSS von der Person, der diese Rolle übertragen werden soll, die Akzeptanz zur Übertragung der Rolle und der damit verbundenen

Verantwortung sowie den daraus resultierenden Pflichten zur Gewährleistung der Sicherheit eingeholt werden.

Darüber hinaus MUSS sichergestellt werden, dass durch die Übertragung einer Rolle keine Interessenskonflikte entstehen und die Unabhängigkeit gewahrt ist, d.h. dass

- die Bereiche, die mit der Generierung und Sperrung von Zertifikaten betraut sind, bei ihren Entscheidungen über die Einrichtung, Bereitstellung, Aufrechterhaltung und Aussetzung von Trust Services in Übereinstimmung mit den geltenden Zertifikatsrichtlinien unabhängig von anderen Organisationen sein MÜSSEN,
- alle Mitarbeiter, die mit der Generierung und Sperrung von Zertifikaten betraut sind, in der Ausübung ihrer Tätigkeit frei von finanziellem oder anderem Druck sein MÜSSEN, der das Vertrauen in die Trust Services beeinträchtigen könnte. Dies gilt sowohl für alle Mitarbeiter in vertrauenswürdigen Rollen als auch für die leitenden Angestellten und Führungskräfte.

Die Struktur, die die Unparteilichkeit des Betriebs gewährleistet, MUSS dokumentiert werden.

Die Rolleninhaber MÜSSEN darauf hingewiesen werden, dass Sie nur in der zugewiesenen Rolle handeln dürfen, wenn Sie Aufgaben ausführen, die der Rolle zugewiesen sind.

Die Vergabe der erforderlichen Berechtigungen MUSS nach dem „Least Privilege“-Prinzip erfolgen, d.h. alle Berechtigungen MÜSSEN auf das erforderliche Minimum beschränkt werden.

Nach Beendigung des Arbeitsverhältnisses eines Mitarbeiters in einer vertrauenswürdigen Rolle MÜSSEN dessen Zugriffsberechtigungen innerhalb von 24 Stunden entzogen werden.

Wenn vertrauenswürdige Rollen oder Teile davon an Dritte übertragen werden (z.B. externe RA, siehe Kap. 1.3.2), MÜSSEN die Verantwortlichkeiten und Regelungen klar definiert und entsprechende Vereinbarungen mit den Dritten getroffen werden, um sicherzustellen, dass alle vom TSP vorgegebenen Regelungen auch von den Dritten eingehalten werden.

5.2.4 Rollen, die eine Aufgabentrennung erfordern

In Konflikt stehende Aufgaben und Verantwortungsbereiche MÜSSEN voneinander getrennt werden.

Folgende Rollen MÜSSEN voneinander getrennt werden:

- Leiter Trust Center und/oder Leiter VDA
- Trust Center Information Security Officer und/oder interner Auditor
- Registrierungsmitarbeiter
- Administrator

Darüber hinaus DÜRFEN Personen in o.g. Rollen NICHT gleichzeitig auch Antragsteller für Endteilnehmer-Zertifikate sein. Ausgenommen davon sind

- Anträge für eigene Zertifikate des TSP sowie Zertifikate für Mitarbeiter des TSP,
- Anträge für eigene Zertifikate einer Organisation, die eine externe Registrierungsstelle betreibt, sowie Zertifikate für Mitarbeiter dieser Organisation.

Ausnahmen MÜSSEN in den CPS beschrieben werden.

5.3 Personelle Maßnahmen

5.3.1 Qualifikationen, Erfahrung und Freigaben

Das Management der TSP MUSS über

- Erfahrung oder Schulung in Bezug auf die angebotenen Dienste des TSP,
- Vertrautheit mit Sicherheitsverfahren für Personal mit Sicherheitsverantwortung und
- Erfahrung mit Informationssicherheit und Risikobewertung, die ausreicht, um Managementfunktionen auszuführen

verfügen.

Die Mitarbeiter der TSP MÜSSEN aufgrund ihrer Erfahrung und/oder geeigneten Schulungen über hinreichendes Expertenwissen und Qualifikationen für die Ausübung ihrer Tätigkeit verfügen. Darüber hinaus MÜSSEN die Mitarbeiter für die Ausübung ihrer Tätigkeit angemessen zu allgemeinen Sicherheits- und Datenschutzbestimmungen sowie den konkreten Vorgaben des ISMS des TSP geschult sein.

Die Mitarbeiter des TSP, die mit der Überprüfung von Identitätsdokumenten im Rahmen der Identifizierungsprozesse betraut sind, MÜSSEN bzgl. der Erscheinungsbilder und Validierungen der akzeptierten Identitätsdokumente geschult sein und Zugang zu einschlägigen Informationsquellen haben.

5.3.2 Verfahren zur Hintergrundprüfung

Vor der Einstellung einer Person MUSS dessen Identität und Vertrauenswürdigkeit überprüft werden.

[EVCP] Personen, die mit einer vertrauenswürdigen Rolle betraut werden sollen, MÜSSEN persönlich unter Vorlage eines amtlichen Ausweises identifiziert werden und eine Hintergrundüberprüfung durchlaufen, in der

- die vorherige Beschäftigung,
- die beruflichen Referenzen,
- der Bildungsabschluss sowie
- ein amtliches Führungszeugnis

geprüft werden.

[QCP] Die Zuverlässigkeit des Personals MUSS durch regelmäßige Vorlage amtlicher Führungszeugnisse geprüft werden.

[3145] Personen, welche mit kritischen oder sicherheitsrelevanten Prozessen betraut werden sollen, MÜSSEN erfolgreich eine Sicherheitsüberprüfung absolviert haben.

Personen, die für eine Straftat verurteilt worden sind, welche die Eignung für die vorgesehene Rolle beeinträchtigt, DÜRFEN NICHT mit dieser Rolle betraut werden.

[VS-NfD] Die o.g. Sicherheitsüberprüfung nach [3145] MUSS mindestens gemäß [SÜG] Level Ü1 absolviert werden.

5.3.3 Schulungsanforderungen

Keine Vorgabe (siehe dazu Kap. 5.3.1).

[TLS] [SMIME] Alle RA-Mitarbeiter MÜSSEN zu folgenden Themen geschult werden:

- Grundlegende Kenntnisse zu PKI, Authentifizierungs- und Überprüfungsrichtlinien und -verfahren
- Allgemeine Bedrohungen für den Informationsüberprüfungsprozess, einschließlich Phishing und Social Engineering
- Relevante CP und/oder CPS sowie die [BR], [SBR] und ggf. [EVCG]

Zu diesen Schulungen MÜSSEN Nachweise geführt werden und es MUSS dokumentiert werden, dass jeder mit der Validierung betraute Mitarbeiter über das erforderliche Knowhow verfügt, bevor dieser die Tätigkeiten übernimmt.

Darüber hinaus MUSS von allen RA-Mitarbeitern verlangt werden, dass sie eine vom TSP bereitgestellte Prüfung der in den [BR], [SBR] und ggf. [EVCG] aufgeführten Anforderungen zur Validierung von Informationen bestehen.

5.3.4 Nachschulungsintervalle und -anforderungen

Personen in vertrauenswürdigen Rollen SOLLTEN regelmäßig (mindestens jährlich) zu aktuellen Bedrohungen und Sicherheitspraktiken geschult werden.

Durch geeignete regelmäßige Schulungen MUSS sichergestellt werden, dass Personal in vertrauenswürdigen Rollen das erforderliche Knowhow dauerhaft aufrechterhält.

5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Keine Vorgabe.

5.3.6 Sanktionen bei unbefugten Handlungen

Das Personal des TSP MUSS rechenschaftspflichtig für sein Handeln sein und bei Verstößen gegen die Vorgaben sanktioniert werden.

5.3.7 Anforderungen an unabhängige Auftragnehmer

Die in Kap. 5.3 aufgeführten Anforderungen gelten, sofern anwendbar, analog für beauftragte Dritte.

[TLS] [SMIME] An der Ausstellung von Zertifikaten beteiligtes Personal Dritter MUSS bzgl. der Einhaltung der Schulungs- und Qualifikationsanforderungen gemäß Kap. 5.3.1 und 5.3.3 überprüft werden.

5.3.8 Dokumentation, die dem Personal zur Verfügung gestellt wird

Den Rolleninhabern MÜSSEN Rollenbeschreibungen zur Verfügung gestellt werden, welche unter Berücksichtigung der zuvor aufgeführten Anforderungen (Kap. 5.3) die sich aus sich aus der jeweiligen Rolle ergebenden Verantwortungen und Pflichten beschreiben.

Diese Rollenbeschreibungen MÜSSEN, wo erforderlich, zwischen allgemeinen und TSP-spezifischen Rollen unterscheiden.

Die in der Informationssicherheitsrichtline festgelegten Sicherheitsrollen und -zuständigkeiten MÜSSEN in Arbeitsplatzbeschreibungen oder in Dokumenten beschrieben werden, die allen betroffenen Mitarbeitern zur Verfügung stehen.

5.4 Protokollierungsverfahren

5.4.1 Zu protokollierende Ereignisse

Die folgenden Ereignisse MÜSSEN inkl. Angabe der präzisen Zeit, sofern anwendbar der Identität des Auslösers und der Beschreibung des Ereignisses in den jeweiligen Systemlogs protokolliert werden:

- Alle wesentlichen Ereignisse der Zertifikats- und Schlüsselmanagementsysteme sowie der Statusdienste, das sind, sofern anwendbar, mindestens:
  - Schlüsselerzeugung, -sicherung, -speicherung, -wiederherstellung, -archivierung und -Vernichtung,
  - Zertifikatsbeantragung inkl. Erneuerung,
  - Validierungen, Genehmigungen und Ablehnungen,
  - Ausstellung der Zertifikate,
  - Beantragung von Sperrungen,
  - Sperrung von Zertifikaten,
  - Generierung von Sperrlisten und
  - Signatur von OCSP-Antworten.
- Alle sicherheitsrelevanten Ereignisse an den PKI- und Sicherheitssystemen, das sind insbesondere:
  - Änderungen der Sicherheitsrichtlinien der Systeme,
  - das Starten und Herunterfahren der Systeme,
  - Systemabstürze und Hardwarefehler,
  - Uhrzeitsynchronisationsereignisse,
  - Firewall- und Router-Aktivitäten sowie
  - erfolgreiche und nicht erfolgreiche PKI-Systemzugriffsversuche.
- Installation, Update und Deinstallation von Software auf den PKI-Systemen.

Darüber hinaus MÜSSEN in den Zutrittssystemen alle physikalischen Ein- und Austritte in bzw. aus den Sicherheitszonen protokolliert werden.

5.4.2 Häufigkeit der Log-Verarbeitung

Die Logdaten MÜSSEN wie folgt ausgewertet werden:

- Sicherheitsrelevante Ereignisse MÜSSEN wie in Kap. 6.6.2 beschrieben ausgewertet werden.
- Alle anderen Logdaten MÜSSEN nur im Bedarfsfall ausgewertet werden, z.B. bei Fehlerbehebungs- oder Analysetätigkeiten.

5.4.3 Aufbewahrungszeitraum für Logdaten

Die Logdaten MÜSSEN über einen angemessenen Zeitraum aufbewahrt werden, die Aufbewahrungsdauern MÜSSEN in den CPS beschrieben werden.

[TLS] [SMIME] Die Logdaten MÜSSEN für mindestens zwei Jahre nach ihrem Eintreten aufbewahrt werden.

5.4.4 Schutz der Audit-Protokolle

Logdaten MÜSSEN vertraulich und integritätsgesichert aufbewahrt und so geschützt werden, dass diese nicht einfach zerstört oder gelöscht werden können, siehe dazu auch Kap. 5.4.6.

Logdaten MÜSSEN im Bedarfsfall bereitgestellt werden, z.B. in Gerichtsverfahren oder auf Anfrage interner und externer Auditoren.

Die Aufbewahrung der Logdaten MUSS überwacht werden (z.B. in internen Audits).

5.4.5 Backup-Verfahren für Audit-Protokolle

Keine Vorgabe.

5.4.6 Audit-Sammelsystem

Die Logdaten MÜSSEN in einem separaten manipulationssicheren System, d.h. nicht nur in dem System, in dem die Ereignisse protokolliert werden, gesammelt werden. Das System MUSS so gestaltet sein, dass Einträge nur hinzugefügt, jedoch nicht während der festgelegten Aufbewahrungsdauer gelöscht werden können, die Speicherkapazität des Systems MUSS dementsprechend ausgelegt sein.

5.4.7 Benachrichtigung der Person, die ein Ereignis ausgelöst hat

Keine Vorgabe.

5.4.8 Nutzung von Protokolldaten zur Schwachstellenprüfung

Keine Vorgabe.

5.5 Aufbewahrung von Aufzeichnungen

5.5.1 Aufzubewahrende Aufzeichnungen

Zu jedem Zertifikat MUSS die Antrags-/Zertifikatshistorie mit Angabe von Datum, Uhrzeit und, sofern anwendbar, der Identität der handelnden Person aufgezeichnet werden. Dazu zählen die folgenden Aktivitäten der Zertifikatsnehmer sowie der internen und ggf. externen RAs:

- Alle Aktivitäten im Zusammenhang mit der Beantragung, Registrierung, Validierung und Genehmigung oder Ablehnung von Anträgen auf Ausstellung, Erneuerung und Sperrung von Zertifikaten aller Hierarchiestufen
- Alle Aktivitäten im Zusammenhang mit dem Lebenszyklus von Schlüsseln und Zertifikaten aller Hierarchiestufen. Dazu zählen mindestens, sofern anwendbar,
  - die Generierung, Speicherung, Backup, Wiederherstellung, Archivierung und Zerstörung von Schlüsseln inkl. der Vorbereitung bzw. Bereitstellung von QSCD oder anderen kryptografischen Geräten sowie
  - die Ausstellung, Akzeptanz, Veröffentlichung und Sperrung von Zertifikaten.

Des Weiteren MÜSSEN zu jedem Zertifikat die im Rahmen der Beantragung einer Ausstellung, Erneuerung, Änderung oder Sperrung vom Antragsteller vorgelegten oder dem Antragsteller übermittelten relevanten Informationen und Dokumente aufgezeichnet bzw. aufbewahrt werden („Registrierungsinformationen“). Hierzu zählen mindestens:

- Informationen zur Identität und ggf. weiterer Attribute des Zertifikatsnehmers, einschließlich, sofern anwendbar, einem Verweis auf die für die Überprüfung verwendeten Unterlagen bzw. Quellen
  Anm.: Sofern die Identität oder Attribute anhand einer öffentlichen und auf Dauer zugänglicher Quelle überprüft wurden, genügt die Information, welche Quelle verwendet wurde und ob die Daten übereinstimmten. Ein Auszug aus der Quelle muss nicht aufbewahrt werden.
- Die ggf. mit dem Zertifikatsnehmer abgeschlossene Vereinbarung, mindestens jedoch Akzeptanz der zum Zeitpunkt der Antragstellung geltenden Nutzungsbedingungen

[SIV] [SSV] Im Falle von VDA-Ident MÜSSEN ergänzend zu o.g. Aufzeichnungen von dem geprüften Identitätsdokument der Aussteller, die Gültigkeitsdauer und die eindeutige Nummer aufgezeichnet werden.

Darüber hinaus MÜSSEN folgende Informationen und Dokumente aufgezeichnet bzw. aufbewahrt werden:

- Alle veröffentlichten CP, CPS und Nutzungsbedingungen
- Zertifizierungsunterlagen und Auditberichte
- relevante Dokumentationen bzgl. der Sicherheit der Systeme aus dem
  - Changemanagement,
  - Schwachstellenmanagement,
  - Rollenmanagement sowie dem
  - Lifecycle-Management der kryptografischen Module.
- Ggf. weitere Informationen, die zur Gewährleistung der Kontinuität der Dienste erforderlich sind oder als Beweismittel in Gerichtsverfahren benötigt werden

Unter Berücksichtigung der relevanten Datenschutzaspekte DÜRFEN weitere Daten aufgezeichnet werden. In den CPS sowie den Nutzungsbedingungen MUSS beschrieben werden, welche Daten aufgezeichnet werden.

[TLS] [SMIME] Zu jedem Zertifikat MUSS darüber hinaus die verwendete Methode zur Validierung des Domain-Namens, der IP-Adresse oder der Mail-Adresse gemäß [BR#3.2.2.4], [BR#3.2.2.5] bzw. [SBR#3.2.2] inkl. der der Validierung zugrundeliegenden Version der [BR] bzw. [SBR] aufgezeichnet werden.

[3145] Die Aufzeichnungen MÜSSEN so archiviert werden, dass alle ausgestellten Zertifikate eindeutig einem registrierten Antragsteller zugeordnet werden können. Darüber hinaus MUSS eine Nachverfolgung möglich sein, um zu verhindern, dass betrügerische oder manipulierte Zertifikate erzeugt werden.

5.5.2 Aufbewahrungszeitraum für Aufzeichnungen

Neben den Zertifikaten selbst MÜSSEN die folgenden der in Kap. 5.5.1 aufgeführten Aufzeichnungen für mindestens 7 Jahre nach Ablauf der Gültigkeit der betroffenen Zertifikate archiviert werden:

- Antrags-/Zertifikatshistorie
- Registrierungsinformationen
- CP, CPS und Nutzungsbedingungen
- Zertifizierungsunterlagen und Auditberichte

Alle anderen Unterlagen MÜSSEN für mindestens 2 Jahre aufbewahrt werden.

Die Aufbewahrungszeiträume (ggf. je Zertifikatstyp) MÜSSEN in den CPS sowie den Nutzungsbedingungen beschrieben werden.

Die Pflicht zur Aufbewahrung der Aufzeichnungen gilt auch über die Beendigung eines Trust Services hinaus. Im Beendigungsplan MUSS daher festgelegt werden, welche Informationen wohin übergeben werden und wie auf diese Informationen zugegriffen werden kann, siehe dazu auch Kap. 5.8.

[QCP-l] [QCP-n] Die Zertifikatshistorie sowie die Registrierungsinformationen MÜSSEN dauerhaft aufbewahrt werden.

5.5.3 Schutz der Aufzeichnungen

Aufzeichnungen MÜSSEN vertraulich und integritätsgesichert aufbewahrt und so geschützt werden, dass diese nicht einfach zerstört oder gelöscht werden können.

[EVCP] Die Aufbewahrung der Informationen und Dokumente MUSS überwacht werden (z.B. in internen Audits).

[QCP] Elektronisch aufbewahrte und mittels QES oder Zeitstempel integritätsgesicherte Aufzeichnungen MÜSSEN zur Gewährleistung der langfristigen Beweiserhaltung durch geeignete Maßnahmen neu geschützt werden, wenn der bisherige Schutz im Laufe der Zeit abschwächt.

5.5.4 Backup-Verfahren für Aufzeichnungen

Keine Vorgabe.

5.5.5 Anforderungen an Zeitstempel von Datensätzen

Keine Vorgabe.

5.5.6 Archivsystem (intern oder extern)

Keine Vorgabe.

5.5.7 Verfahren zur Beschaffung und Überprüfung von Aufzeichnungen

Die Aufzeichnungen MÜSSEN im Bedarfsfall ausgewertet und bereitgestellt werden, z.B. bei Problemmeldungen, in Gerichtsverfahren oder auf Anfrage interner und externer Auditoren.

Die Zugriffsmöglichkeiten auf die Archivinformationen MÜSSEN festgelegt und TSP-intern dokumentiert werden.

5.6 Schlüsselwechsel

Vor Ablauf eines CA-Zertifikats MUSS, sofern der betroffene Trust Service fortgesetzt werden soll, rechtzeitig ein neues CA-Zertifikat gemäß den aktuellen Versionen dieser CP und dem CPS ausgestellt werden. Dabei SOLLTE der Zeitraum zwischen der Veröffentlichung des neuen CA-Zertifikats und der Außerbetriebnahme des ablaufenden CA-Zertifikats hinreichend groß gewählt werden, so dass für die Zertifikatsnehmer keine Unterbrechung in deren Betrieb entsteht.

5.7 Kompromittierung und Notfall-Wiederherstellung

5.7.1 Verfahren zur Meldung und Behandlung von Vorfällen und Kompromittierungen

Die Verfahren zur Meldung und Behandlung von Vorfällen und Kompromittierungen sowie zur Wiederherstellung nach Ausfällen oder Katastrophen MÜSSEN in der Notfalldokumentation beschrieben werden.

Die Notfalldokumentation MUSS folgende Aspekte beinhalten:

- Notfallvorsorge
  - Vorgaben zum Backup kritischen kryptografischen Materials an einem anderen Standort,
  - Vorgaben zum regelmäßigen Backup aller relevanten Daten, die zur Wiederaufnahme des CA-Betriebs nach einem Notfall erforderlich sind, an sicheren, vorzugsweise entfernt auseinander liegenden Orten,
  - Entfernung des Hauptstandorts zu den Standorten, die zur Wiederherstellung des Geschäftsbetriebs genutzt werden können,
- Benennung aller beteiligten Rollen und Eskalationsstufen,
- Verantwortung aller Beteiligten,

- Voraussetzungen, unter denen aus einem Vorfall ein Notfall wird,
- Notfallprozesse,
- Rückfall-Prozesse,
- Wiederaufnahmeverfahren,
- Prozesse zur Meldung
  - von Sicherheitsverletzungen an die zuständigen Aufsichtsbehörden (innerhalb von 24 Stunden) oder sonstige relevanten Beteiligten,
  - von Sicherheitsverletzungen, die sich nachteilig auf Person oder Organisationen auswirken, an die Betroffenen (unverzüglich),
  - von Datenschutzvorfällen an die zuständigen Behörden oder sonstige relevanten Beteiligten (innerhalb von 24 Stunden),
- Zielvorgaben für die Wiederherstellungszeit,
- Nachbereitung inkl. Ursachenermittlung zur Vermeidung von Wiederholungen,
- Review Zyklen des Notfallplans (mindestens jährlich),
- Sensibilisierungs- und Schulungsanforderungen,
- Regelmäßige Notfallübungen (mindestens jährlich),
- Plan zur Wiederherstellung des Betriebs nach Unterbrechung oder Ausfall kritischer Geschäftsprozesse,
- Festlegung akzeptabler Ausfall- und Wiederherstellungszeiten,
- Verfahren zur größtmöglichen Sicherung des beeinträchtigten Standorts während des Zeitraums nach einem Notfall und vor der Wiederherstellung am ursprünglichen oder an einem anderen Standort.

Die Notfalldokumentation MUSS den Auditoren auf Anfrage offengelegt werden.

Die Verfahren zur Meldung von Vorfällen MÜSSEN festgelegt werden und es MUSS sichergestellt werden, dass diese den Mitarbeitern bekannt sind und genutzt werden.

Zur Minimierung möglicher Schäden MUSS in angemessener Zeit auf Vorfälle, die von Personen gemeldet werden und auf Alarme, die von den Systemen gemeldet werden (siehe Kap. 6.6.2) reagiert werden. Potenziell sicherheitskritischen Vorfällen MUSS unverzüglich durch Mitarbeiter in vertrauenswürdigen Rollen nachgegangen werden.

[TLS] [SMIME] Verstöße gegen die relevanten Root Store Policies MÜSSEN unverzüglich den entsprechenden Root-Store-Betreibern gemeldet werden und es SOLLTE die Ausgabe der betroffenen Zertifikatstypen eingestellt werden, bis die Ursache für den Verstoß behoben ist.

[VS-NfD] Der Notfallplan MUSS vom Sicherheitsbeauftragten freigegeben werden.

5.7.2 Wiederherstellung bei Beschädigung von Computern, Software oder Daten

Siehe Kap. 5.7.1.

5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln

Die Kompromittierung, der Verdacht auf Kompromittierung und der Verlust eines privaten CA-Schlüssels MÜSSEN als Notfall in der Notfalldokumentation festgelegt werden und die daraus resultierenden Aktivitäten MÜSSEN beschrieben werden.

Im Falle einer Kompromittierung eines CA-Schlüssels MUSS das korrespondierende CA-Zertifikat gesperrt werden und alle Betroffenen (Zertifikatsnehmer sowie alle Weiteren, mit denen

die TSP Vereinbarungen getroffen haben) informiert werden. Darüber hinaus MUSS vertrauenden Dritten die Informationen verfügbar gemacht werden und angezeigt werden, dass den von der betroffenen CA ausgestellten Zertifikaten und Statusauskünften nicht mehr vertraut werden kann.

Des Weiteren SOLLTEN alle Endteilnehmer-Zertifikate (mit Ausnahme von Kurzzeitzertifikaten) gesperrt werden.

[QCP] Die Verfahren zur Bereitstellung der Statusinformationen zu Endteilnehmer-Zertifikaten im Falle der Kompromittierung eines CA-Schlüssels MÜSSEN in den CPS beschrieben werden.

[3145] Im Falle des Verdachts einer Kompromittierung eines CA-Schlüssels DÜRFEN die betroffenen Schlüssel bis zur endgültigen Klärung NICHT mehr benutzt werden.

5.7.4 Geschäftsfortführung nach einem Notfall

Im Falle eines Notfalls MUSS der Betrieb innerhalb der in der Notfalldokumentation festgelegten Frist wiederhergestellt werden, nachdem alle Ursachen durch geeignete Abhilfemaßnahmen beseitigt wurden.

5.8 Einstellung des CA oder RA Betriebes

Bei Beendigung eines Trust Services MÜSSEN potenzielle Störungen für Zertifikatsnehmer und Zertifikatsnutzer soweit möglich minimiert werden.

Sofern möglich, SOLLTE die Bereitstellung des Trust Services für bestehende Kunden an einen anderen TSP übertragen werden, ansonsten MUSS eine sichere Beendigung des Trust Service gewährleistet sein.

Vor der Beendigung oder Übertragung eines Trust Services MÜSSEN

- alle Betroffenen informiert werden (Zertifikatsnehmer, ggf. zuständige Aufsichtsbehörden, betroffene Root Store Betreiber oder weitere Betroffene, mit denen der TSP Verträge hat),
- vertrauenden Dritten die Information über die Beendigung oder Übertragung bereitgestellt werden,
- die Vereinbarungen mit Unterauftragnehmern, z.B. externen RAs, beendet werden.

Vor der Beendigung eines Trust Service MÜSSEN

- eine zuverlässige Stelle verpflichtet werden, alle Informationen, die erforderlich sind, um den Betrieb des Trust Service nachzuweisen, für einen angemessenen und ggf. mit den Zertifikatsnehmern und Anderen vereinbarten Zeitraum aufzubewahren. Dazu zählen mindestens:
  - Registrierungsinformationen
  - Zertifikatsstatusinformationen
  - Ereignisprotokollarchive
  - CA-Zertifikate
- die privaten CA-Schlüssel zerstört oder so außer Betrieb genommen werden, dass diese nicht wiederverwendet werden können und
- alle noch gültigen und nicht gesperrten Zertifikate gesperrt werden.

Vor Übertragung eines Trust Services MÜSSEN mit dem übernehmenden TSP entsprechende Vereinbarungen abgeschlossen werden.

Nach der Beendigung oder Übertragung eines Trust Services und Übergabe der Informationen an eine andere Stelle MÜSSEN alle Schlüssel, Zertifikate und Kundendaten gelöscht werden.

Die Vorkehrungen, die zur Beendigung oder Übertragung eines Trust Services getroffen werden, MÜSSEN in einem aktuellen Beendigungsplan festgelegt werden.

Des Weiteren MUSS in den CPS beschrieben werden, wie bei Beendigung eines Trust Services verfahren wird, mindestens sind das

- die Information aller Betroffenen,
- der Umgang mit Statusauskünften zu nicht abgelaufenen Zertifikaten und
- sofern anwendbar, die Übertragung der Pflichten an Andere.

[QCP] In den CPS MÜSSEN darüber hinaus die Verfahren zur Bereitstellung der Statusinformationen für alle abgelaufenen Zertifikate gemäß Kap. 4.10 beschrieben werden.

[QCP-l] [QCP-n] In dem Beendigungsplan MUSS berücksichtigt werden,

- dass die Zertifikatsnehmer, soweit möglich zwei Monate im Voraus über die Beendigung und die Übergabe der Zertifikate informiert werden,
- dass alle Zertifikate, deren Statusinformationen sowie die relevanten Informationen gemäß Kap. 5.5.1 möglichst in elektronischer Form nach dem Stand der Technik entweder einem anderen qualifizierten TSP oder der Bundesnetzagentur als zuständige Aufsichtsbehörde übergeben werden.

Als Sperrgrund für die gesperrten Endteilnehmer-Zertifikate MUSS `cessationOfOperation` in den Statusdiensten aufgeführt werden.

Vor Beendigung einer RA MUSS festgelegt und in den CPS beschrieben werden, welche Informationen (z.B. bei der RA aufbewahrte oder archivierte Zertifikatsanträge oder sonstige Registrierungsinformationen) dem TSP übergeben werden müssen.

6 TECHNISCHE SICHERHEITSMAßNAHMEN

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren

Alle Schlüssel MÜSSEN den in Kap. 6.1.5 und 6.1.6 aufgeführten Algorithmen, Schlüssellängen und Qualitätsanforderungen genügen. Die Schlüssel MÜSSEN für die gesamte Lebensdauer und die beabsichtigten Verwendungszwecke zum Zeitpunkt der Genration als geeignet angesehen werden.

6.1.1.1 Generierung von CA-Schlüsselpaaren

CA-Schlüsselpaare MÜSSEN in einem Kryptomodul gemäß Kap. 6.2.1 in der sicheren Umgebung des Trust Centers in einer Schlüsselzeremonie generiert werden. Es MUSS sich dabei um das Kryptomodul handeln, in dem später der private Schlüssel verwendet wird, so dass kein Im- oder Export der Schlüssel außer zu Backup-Zwecken erforderlich ist.

Die beteiligten Rollen sowie deren Aufgaben und Verantwortlichkeiten vor, während und nach der Schlüsselzeremonie MÜSSEN festgelegt und dokumentiert sein.

Die einzelnen Schritte der Schlüsselzeremonie MÜSSEN einem festgelegten Protokoll folgen und in diesem dokumentiert werden.

Die Generierung MUSS durch mindestens zwei Mitarbeiter des TSP in vertrauenswürdigen Rollen erfolgen.

Zur Generierung von Root-CA-Schlüsseln gelten dabei folgende Anforderungen:

- Jeder der beiden Mitarbeiter MUSS Kenntnis von nur einem Teil der zur Schlüsselgenerierung erforderlichen Aktivierungsdaten.
- Die beiden Mitarbeiter MÜSSEN in unterschiedlichen Rollen agieren.

Zur Generierung von Sub-CA-Schlüsseln gilt dabei folgende Anforderung:

- Zum Nachweis der Authentizität und der Integrität MUSS der Hashwert des generierten öffentlichen Schlüssels oder des CSR, der den öffentlichen Schlüssel beinhaltet, im Generierungsprotokoll aufgenommen und bei der Zertifikatsbeantragung (siehe Kap. 4.1) übergeben werden.

Ein interner Auditor (siehe Kap. 8.2) MUSS die Schlüsselzeremonie überwachen und deren korrekte Durchführung im Protokoll bestätigen.

[TLS] [SMIME] Sowohl ein interner als auch ein qualifizierter externer Auditor (siehe Kap. 8.2) MÜSSEN die Schlüsselzeremonie überwachen und deren korrekte Durchführung im Protokoll bestätigen.

6.1.1.2 Generierung von OCSP-Signer-Schlüsselpaaren

OCSP-Signer Schlüsselpaare MÜSSEN in kryptografischen Modulen gemäß Kap. 6.2.1 generiert werden, es MUSS sich dabei um das Kryptomodul handeln, in dem später der private Schlüssel verwendet wird, so dass kein Im- oder Export der Schlüssel außer zu Backup-Zwecken erforderlich ist.

6.1.1.3 Generierung von RA-Schlüsselpaaren

RA Schlüsselpaare MÜSSEN in kryptografischen Modulen gemäß Kap. 6.2.1 generiert werden.

6.1.1.4 Generierung von Endteilnehmer-Schlüsselpaaren

Endteilnehmer-Schlüsselpaare DÜRFEN entweder durch die Sub-CA, den Zertifikatsnehmer selbst oder delegierte Dritte generiert werden.

Wenn Endteilnehmer-Schlüsselpaare durch die Zertifikatsnehmer generiert werden, so MÜSSEN die Zertifikatsnehmer über die zu verwendenden zulässigen Algorithmen und Schlüssellängen informiert werden.

Wenn Endteilnehmer-Schlüsselpaare durch die Sub-CA erzeugt werden, so MÜSSEN die Schlüssel auf eine sichere Art und Weise generiert werden und bis zur Zertifikatserzeugung vorgehalten werden, so dass die Integrität und Vertraulichkeit sichergestellt werden.

[TLS] Endteilnehmer-Schlüsselpaare DÜRFEN NICHT durch die Sub-CA generiert werden.

[QCP-n-qscd] [QCP-l-qscd] Endteilnehmer-Schlüsselpaare MÜSSEN durch ein zertifiziertes QSCD (siehe Kap. 6.2.1) erzeugt werden.

[3145] Wenn Endteilnehmer-Schlüsselpaare für kryptografische Token als Speichermedium von der Sub-CA generiert werden,

- SOLLTEN die Schlüssel durch den Token selbst generiert werden,
- MÜSSEN außerhalb des Tokens erzeugte Schlüssel sofort nach dem Einbringen in den Token gelöscht werden, sofern keine Sicherung der Schlüssel angeboten wird.

6.1.2 Bereitstellung der privaten Schlüssel an die Zertifikatsnehmer

Die Verfahren zur Übergabe der Schlüssel MÜSSEN in den Nutzungsbedingungen und den CPS beschrieben werden.

Wenn Endteilnehmer-Schlüsselpaare vom TSP generiert werden, MÜSSEN folgende Vorgaben berücksichtigt werden:

- Die Schlüssel MÜSSEN dem Zertifikatsnehmer so übergeben werden, dass die Wahrung der Vertraulichkeit und Integrität sichergestellt und eine unautorisierte Nutzung ausgeschlossen ist, es sei denn die TSP verwalten die Schlüssel im Auftrag des Zertifikatsnehmers.
- Nach der Übergabe der Schlüssel an den Zertifikatsnehmer MÜSSEN alle Kopien der Schlüssel in den Systemen des TSP gelöscht werden, es sei denn die Schlüssel sollen im Auftrag des Zertifikatsnehmers beim TSP hinterlegt werden (siehe Kap. 6.2.3).

[NCP] Wenn Endteilnehmer-Schlüsselpaare vom TSP generiert und im Auftrag des Zertifikatsnehmers verwaltet werden und die Schlüsselverwendung in den korrespondierenden Zertifikaten mit `nonRepudiation` festgelegt ist, MUSS sichergestellt werden, dass die Zertifikatsnehmer die alleinige Kontrolle über die Schlüssel haben.

Für den Fall, dass ein anderer TSP als der, der die Schlüssel generiert und die Zertifikate ausgestellt hat, Endteilnehmer-Schlüssel im Auftrag der Zertifikatsnehmer verwaltet und die Schlüsselverwendung in den korrespondierenden Zertifikaten mit `nonRepudiation` festgelegt ist, MUSS der TSP, der die Schlüssel generiert und die Zertifikate ausgestellt hat, sich bestätigen lassen, dass der die Schlüssel verwaltende TSP sicherstellt, dass die Zertifikatsnehmer die alleinige Kontrolle über die Schlüssel haben.

Die Konformität zu [ETS431-1] SOLLTE verwendet werden, um nachzuweisen, dass ein TSP, der Schlüssel im Auftrag der Zertifikatsnehmer verwaltet, die Anforderungen zur Gewährleistung der alleinigen Kontrolle über die Schlüssel erfüllt.

[NCP+] Wenn Endteilnehmer-Schlüsselpaare vom TSP generiert werden, MUSS sichergestellt werden, dass diese auf sicheren kryptografischen Geräten (z.B. Smartcards) auf sichere Art und Weise den registrierten Zertifikatsnehmern übergeben werden. Für den Fall, dass ein Zertifikatsnehmer seine Schlüssel von einem anderen TSP als dem, der die Schlüssel generiert und die Zertifikate ausgestellt hat, verwalten lässt, muss das Gerät diesem TSP auf sicherem Weg übergeben werden.

[QCP-n-qscd] [QCP-l-qscd] Die privaten Schlüssel MÜSSEN den Zertifikatsnehmern in zertifizierten QSCD gemäß Kap. 6.2.1 übergeben oder vom TSP im Auftrag der Zertifikatsnehmer verwaltet werden.

Wenn ein TSP QSCDs von Zertifikatsnehmern verwaltet, MUSS die alleinige Kontrolle der Zertifikatsnehmer über ihre QSCD sichergestellt werden.

[3145] Die Verfahren zur Ausgabe der Token MÜSSEN in den Nutzungsbedingungen und den CPS beschrieben werden.

Wenn die TSP die Endteilnehmer-Schlüssel generieren, MUSS

- sichergestellt werden, dass die Schlüssel dem korrekten Zertifikatsnehmer übermittelt werden,
- sichergestellt werden, dass die Vertraulichkeit der Schlüssel während der Übermittlung gewährleistet ist,
- sichergestellt werden, dass die Schlüssel beim TSP nach der Übermittlung an den korrekten Zertifikatsnehmer gelöscht werden, es sei denn, der TSP bietet ein Schlüsselbackup für die Zertifikatsnehmer an.

[SMIME] Wenn Endteilnehmer-Schlüsselpaare vom TSP oder delegierten Dritten generiert werden, DÜRFEN die privaten Schlüssel NICHT im Klartext gespeichert werden.

6.1.3 Übergabe öffentlicher Schlüssel an die TSP

Keine Vorgabe.

[TLS] Die Formate und die Methoden der akzeptierten CSR SOLLTEN in den CPS oder dort referenzierten Dokumenten festgelegt werden.

6.1.4 Bereitstellung der öffentlichen CA-Schlüssel

CA-Zertifikate MÜSSEN allgemein zugänglich in integrer und authentischer Form bereitgestellt werden (siehe Kap. 2.2).

Bei Root-CA-Zertifikaten MÜSSEN zusätzlich weitere Prüfmechanismen angeboten werden, wie z.B. eine Prüfmöglichkeit des Hashwerts des Zertifikats gegen eine vertrauenswürdige Quelle.

6.1.5 Schlüssellängen

Schlüssel aller Zertifikate aller Hierarchieebenen MÜSSEN den Anforderungen aus [SOGIS] genügen.

Derzeit MÜSSEN folgende Mindestanforderungen beachtet werden:

- RSA: Die Schlüssel SOLLTEN eine Länge von mindestens 3.000 Bit haben (Recommendation gem. [SOGIS]). Schlüssel mit einer Länge von mehr als 1.900 Bit und weniger als 3.000 Bit DÜRFEN noch bis 2025 verwendet werden (Legacy gem. [SOGIS]).
- ECC: Es SOLLTEN Schlüssel aus folgenden Kurven verwendet werden (Recommendation gem. [SOGIS]):
  - BrainpoolP256r1
  - BrainpoolP384r1
  - BrainpoolP512r1
  - NIST P-256
  - NIST P-384
  - NIST P-521

Sollten die verwendeten Schlüssellängen aufgrund neuer Erkenntnisse oder Vorgaben für den Verwendungszweck nicht mehr ausreichen, so MÜSSEN die Zertifikatsnehmer und vertrauende Dritte darüber informiert werden und es MUSS ein Zeitplan zur Sperrung betroffener Zertifikate sowie zur Migration auf hinreichend lange Schlüssel festgelegt werden.

[TLS] [SMIME] Für RSA-Schlüssel gelten folgende Anforderungen:

- sie MÜSSEN mindestens 2048 Bit lang sein
- die Länge des Modulus MUSS durch 8 teilbar sein

EC-Schlüssel MÜSSEN aus folgenden Kurven verwendet werden:

- NIST P-256
- NIST P-384

[VS-NfD] Die Anforderungen aus [TR2102-1] MÜSSEN beachtet werden.

6.1.6 Generierung und Qualitätsprüfung öffentlicher Schlüsselparameter

Keine Vorgabe.

[TLS] [SMIME] Von den Zertifikatsnehmern vorgelegte Schlüssel MÜSSEN auf die Einhaltung folgender Merkmale überprüft werden:

- RSA: Der Wert des Exponenten MUSS eine ungerade Zahl größer oder gleich 3 sein und SOLLTE im Bereich von 2^{16} und 2^{256}-1 liegen.
- RSA: Der Wert des Modulus MUSS eine ungerade Zahl sein, die nicht die Potenz einer Primzahl ist und keine Faktoren hat, die kleiner als 752 sind.
- ECC: Die Schlüssel SOLLTEN entweder mit der ECC-Routine zur vollständigen Validierung öffentlicher Schlüssel oder mit der ECC-Routine zur teilweisen Validierung öffentlicher Schlüssel geprüft werden.

6.1.7 Schlüsselverwendung

Die Verwendung eines privaten Schlüssels MUSS auf die im korrespondierenden Zertifikat in den Attributen `keyUsage` und, sofern vorhanden, `extendedKeyUsage` (siehe Kap. 7.1.2) aufgeführten Verwendungszwecke beschränkt werden.

Die Nutzung der privaten Root-Schlüssel MUSS auf folgende Anwendungsfälle beschränkt werden:

- Signatur des eigenen Root-CA-Zertifikats
- Signatur von Sub-CA-Zertifikaten
- Signatur von OCSP-Signer-Zertifikaten
- Signatur von Sperrlisten

Die Nutzung der privaten Sub-CA-Schlüssel MUSS auf folgende Anwendungsfälle beschränkt werden:

- Signatur von Sub-CA-Zertifikaten
- Signatur von Endteilnehmer-Zertifikaten
- Signatur von OCSP-Signer-Zertifikaten
- Signatur von Sperrlisten
- Signatur von OCSP-Auskünften

6.2 Schutz privater Schlüssel und technische Kontrollen kryptografischer Module

Zum Schutz der privaten Schlüssel aller Hierarchieebenen MÜSSEN hinreichende Sicherheitsmaßnahmen getroffen bzw. den Zertifikatsnehmern vorgegeben werden.

6.2.1 Standards und Kontrollen für kryptografische Module

Die verwendeten kryptografischen Module MÜSSEN entweder nach CC EAL 4 oder höher oder nach einem vergleichbaren Standard evaluiert oder nach FIPS 140-2 Level 3 oder FIPS-140-3 Level 3 zertifiziert sein und gemäß den Vorgaben der Zertifizierungsdokumentation oder in vergleichbarer Konfiguration mit gleichem Sicherheitsniveau betrieben werden.

Manipulationen an kryptografischen Modulen bei Lagerung und Transport MÜSSEN ausgeschlossen werden.

[QCP-n-qscd] [QCP-l-qscd] Die QSCD MÜSSEN den Anforderungen gemäß [eIDAS#Art.29] genügen und gemäß [eIDAS#Art.30] zertifiziert sein.

Der Zertifizierungsstatus der QSCD MUSS bis zum Ablauf der Gültigkeit der Endteilnehmer-Zertifikate gemonitort werden und es MÜSSEN entsprechende Maßnahmen eingeleitet werden, wenn sich der Zertifizierungsstatus vor Ablauf der Endteilnehmer-Zertifikate ändert.

[VS-NfD] Kryptografische Module, in denen CA- und, sofern anwendbar, Endteilnehmer-Schlüsselpaare generiert und betrieben werden, MÜSSEN vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für die VS-NfD-Nutzung zugelassen sein.

6.2.2 Mehrpersonenkontrolle über private Schlüssel (n von m)

Beim Im- und Export von CA-Schlüsseln zu (Rück-)Sicherungszwecken (siehe Kap. 6.2.4 und 6.2.6) MUSS eine Mehrpersonenkontrolle umgesetzt werden.

6.2.3 Hinterlegung privater Schlüssel

Keine Vorgabe.

6.2.4 Sicherung privater Schlüssel

Die privaten CA- und, sofern anwendbar, vom TSP erzeugte Endteilnehmer-Schlüssel, welche gesichert werden sollen, MÜSSEN in einer sicheren Umgebung gesichert werden, dabei MUSS für die Sicherung der Schlüssel bzgl. Zugriff, Manipulation und Verlust das gleiche Sicherheitsniveau wie für die im Betrieb befindlichen privaten Schlüssel erfüllt werden.

Die Sicherung sowie ggf. die Rücksicherung von CA-Schlüsseln MÜSSEN im Rahmen einer Key-Zeremonie erfolgen. Es gelten dabei die gleichen Bedingungen wie bei der Schlüsselgenerierung (siehe Kap. 6.1.1.1 bzw. 6.1.1.2), auf das Beisein eines externen Auditors DARF jedoch verzichtet werden. Darüber hinaus MUSS sichergestellt sein, dass der Zugriff auf die Sicherungen mindestens zwei Mitarbeiter des TSP in vertrauenswürdigen Rollen erfordert.

[3145] Wenn Schlüssel im Auftrag der Zertifikatsnehmer gesichert werden, MÜSSEN

- die Endteilnehmer-Schlüssel unter Verwendung jeweils individueller Geheimnisse, die von der CA selbst generiert werden, verschlüsselt werden,
- die zur Verschlüsselung verwendeten individuellen Geheimnisse ebenfalls verschlüsselt und getrennt von den Endteilnehmer-Schlüsseln sicher gespeichert werden, so dass deren Integrität und Vertraulichkeit gewährleistet ist,
- die Zertifikatsnehmer im Falle eines Rücksicherungswunsches sicher identifiziert werden (in Anlehnung an die Identifizierung bei Antragsstellung, siehe Kap. 4.2.1),
- die Sicherung dem Zertifikatsnehmer so übergeben werden, wie die originalen Schlüssel (siehe Kap. 6.1.2)

[VS-NfD] Wenn Schlüssel im Auftrag der Zertifikatsnehmer gesichert werden,

- MÜSSEN ergänzend zu den o.g. Vorgaben zu [3145] die Wiederherstellungsmaßnahmen und -richtlinien durch den Sicherheitsbeauftragten freigegeben werden und
- DÜRFEN NICHT andere Schlüssel als die Verschlüsselungsschlüssel gesichert werden.

6.2.5 Archivierung privater Schlüssel

Keine Vorgabe.

[TLS] [SMIME] Die privaten Schlüssel einer Sub-CA DRÜFEN NICHT ohne die Erlaubnis des TSP durch andere Parteien archiviert werden. Ebenso DÜRFEN die privaten Endteilnehmer-Schlüssel NICHT ohne dessen Erlaubnis archiviert werden.

6.2.6 Übertragung privater Schlüssel in oder von einem kryptografischen Modul

Der Im- und Export von Schlüsseln MUSS in einer Schlüssel-Zeremonie und mindestens im Vier-Augen-Prinzip erfolgen. Es gelten dabei die gleichen Bedingungen wie bei der Schlüsselgenerierung (siehe Kap. 6.1.1.1 bzw. 6.1.1.2), auf das Beisein eines externen Auditors DARF jedoch verzichtet werden.

Private Schlüssel DÜRFEN NICHT im Klartext exportiert werden, es SOLLTEN die von den kryptografischen Modulen bereitgestellten Funktionen zur Verschlüsselung der exportierten Schlüssel verwendet werden.

[3145] Bei einem Defekt eines kryptografischen Moduls, welches zur Speicherung und Nutzung privater CA-Schlüssel verwendet wird, MÜSSEN die privaten Schlüssel gemäß den o.g. Vorgaben in ein neues kryptografisches Modul übertragen werden.

6.2.7 Speicherung privater Schlüssel in kryptografischen Modulen

Die in den kryptografischen Modulen gespeicherten Schlüssel MÜSSEN mittels der von den kryptografischen Modulen bereitgestellten Funktionen gesichert abgelegt werden.

6.2.8 Methoden zur Aktivierung privater Schlüssel

Die Aktivierung privater CA-Schlüssel MUSS durch Personen in vertrauenswürdigen Rollen mithilfe der vom HSM bereitgestellten Funktionen erfolgen.

Wenn Endteilnehmer-Schlüssel vom TSP erzeugt werden, MUSS sichergestellt werden, dass deren Aktivierung durch die Zertifikatsnehmer auf sichere Art und Weise erfolgt.

[QCP-n-qscd] [QCP-l-qscd] Die Nutzung privater Endteilnehmer-Schlüssel MUSS in der alleinigen Kontrolle des Zertifikatsnehmers liegen, unabhängig davon, ob er die QSCD selbst besitzt oder diese durch einen TSP in seinem Auftrag managen lässt.

6.2.9 Methoden zur Deaktivierung privater Schlüssel

Die Deaktivierung privater CA-Schlüssel MUSS durch Personen in vertrauenswürdigen Rollen mithilfe der vom HSM bereitgestellten Funktionen erfolgen.

Wenn Endteilnehmer-Schlüssel vom TSP erzeugt werden und den Zertifikatsnehmern mittels kryptografischer Module (z.B. Smartcards) übergeben werden, MUSS sichergestellt werden, dass deren Deaktivierung und ggf. Reaktivierung durch die Zertifikatsnehmer auf sichere Art und Weise erfolgen.

6.2.10 Methoden zur Zerstörung privater Schlüssel

Private CA-Schlüssel MÜSSEN am Ende des Lebenszyklus des korrespondierenden CA-Zertifikats, d.h. mit Ablauf der Gültigkeitsdauer, der Sperrung oder der Außerbetriebnahme des CA-Zertifikats oder der Beendigung des Dienstes, zerstört werden. Die Zerstörung der Schlüssel MUSS in einer Schlüssel-Zeremonie erfolgen und alle Kopien der Schlüssel MÜSSEN berücksichtigt werden. Es gelten dabei, sofern anwendbar, die gleichen Anforderungen wie bei der Generierung der Schlüssel (siehe Kap. 6.1.1.1 bzw. 6.1.1.2).

Wenn kryptografische Module außer Betrieb genommen werden, so MÜSSEN alle privaten Schlüssel, die in dem Modul gespeichert sind, zerstört werden.

6.2.11 Bewertung kryptografischer Module

Kryptografische Module MÜSSEN vor der Beschaffung bzgl. ihrer Nutzbarkeit und der Erfüllung aller Anforderungen bewertet werden.

6.3 Andere Aspekte zur Verwaltung von Schlüsselpaaren

6.3.1 Archivierung des öffentlichen Schlüssels

Öffentliche Schlüssel (d.h. Zertifikate) MÜSSEN gemäß Kap. 5.5.2 aufbewahrt werden.

6.3.2 Nutzungsdauer von Zertifikaten und Schlüsselpaaren

Das Gültigkeitsende eines Zertifikats DARF das Gültigkeitsende des Zertifikats der ausstellenden CA nicht überschreiten.

[QCP-n] [QCP-l] Zertifikate DÜRFEN länger gültig sein als das ausstellende CA-Zertifikat.

[TLS] [SMIME] Die Gültigkeitsdauer eines Root-CA-Zertifikats DARF NICHT größer als 25 Jahre sein. Die Gültigkeitsdauer eines Sub-CA-Zertifikats SOLLTE NICHT größer als 10 Jahre und DARF NICHT größer als 20 Jahre sein.

[TLS] Endteilnehmer-Zertifikate SOLLTEN NICHT länger als 397 Tage gültig sein und DÜRFEN NICHT länger als 398 Tage gültig sein.

[SMIME] Endteilnehmer-Zertifikate DÜRFEN folgende Gültigkeitsdauern NICHT überschreiten:

- [Legacy] 1185 Tage (d.h. drei Jahre zzgl. einer Karenzzeit von max. drei Monaten)
- [Multipurpose] [Strict] 825 Tage (d.h. zwei Jahre zzgl. einer Karenzzeit von max. drei Monaten)

[3145] Die Nutzung des privaten Schlüssels einer Sub-CA MUSS, z.B. durch Deaktivierung, verhindert werden, wenn

- dieser erst zu einem definierten Zeitpunkt verwendet werden soll (z.B. für die Zukunft geplante Inbetriebnahme eines neuen Sub-CA-Zertifikats),
- dieser für einen bestimmten Zeitraum aufgrund eines speziellen Anwendungsfalls nicht verwendet werden soll.

6.4 Aktivierungsdaten

6.4.1 Generierung und Installation von Aktivierungsdaten

Die Aktivierungsdaten der HSM MÜSSEN bei Inbetriebnahme der HSM im Vier-Augen-Prinzip im Rahmen eines geregelten Change-Prozesses mittels der von den kryptografischen Modulen bereitgestellten Funktionen generiert und installiert werden.

Wenn Endteilnehmer-Zertifikate auf kryptografischen Modulen (z.B. Smartcards) ausgegeben werden, welche mit individuellen Aktivierungsdaten (z.B. PINs) versehen werden, MÜSSEN die Aktivierungsdaten auf sichere Art und Weise generiert und in den kryptografischen Modulen eingestellt werden.

6.4.2 Schutz der Aktivierungsdaten

Das Wissen über Aktivierungsdaten der HSM MUSS auf Personen in vertrauenswürdigen Rollen beschränkt werden. Der Kreis der wissenden Personen MUSS dabei auf das unbedingt erforderliche Maß eingeschränkt werden.

Wenn Aktivierungsdaten für Endteilnehmer-Schlüssel vom TSP erzeugt werden (siehe Kap. 6.4.1) MÜSSEN diese von der Erzeugung bis zur Übergabe an den Zertifikatsnehmer so geschützt werden, dass deren Integrität und Vertraulichkeit gewahrt bleibt und sie MÜSSEN dem Zertifikatsnehmer getrennt von den Schlüsseln, d.h. zeitversetzt oder über verschiedene Wege übermittelt werden.

6.4.3 Andere Aspekte der Aktivierungsdaten

Keine Vorgabe.

6.5 Computer-Sicherheitskontrollen

6.5.1 Spezifische technische Anforderungen an die Computersicherheit

Anmerkung: Die nachfolgend aufgeführten Anforderungen gelten, sofern anwendbar, analog für vom TSP beauftragte Dritte.

Die für das Zertifikatsmanagement sowie die Status- und Verzeichnisdienste erforderlichen Systeme MÜSSEN dem Schadenspotential entsprechend geschützt werden.

Die Accounts der für den Betrieb der kritischen Systeme erforderlichen vertrauenswürdigen Rollen (siehe Kap. 5.2.1) MÜSSEN so gemanagt werden, dass

- der Zugriff auf die Systeme und Daten auf die für diese Rollen identifizierten und authentifizierten Personen (siehe Kap. 5.2.3) mit den minimal erforderlichen Berechtigungen beschränkt wird,
- sie in angemessener Zeit geändert oder gelöscht werden.

Für die Accounts, welche direkt die Erstellung von Zertifikaten auslösen können, MUSS eine Multi-Faktor-Authentisierung umgesetzt werden.

Die geforderte Trennung von vertrauenswürdigen Rollen (siehe Kap. 5.2.4) MUSS von den Systemen technisch unterstützt werden.

Administrationssysteme, die zur Umsetzung der Sicherheitsrichtlinien verwendet werden, DÜRFEN NICHT für andere Zwecke verwendet werden.

Es MÜSSEN vertrauenswürdige Systeme eingesetzt werden, welche die technische Sicherheit und Zuverlässigkeit der von den Systemen unterstützten Prozesse sicherstellen.

Die CA-, Zertifikatsmanagement-, Sicherheits- und Frontend-Systeme sowie, falls anwendbar, weitere interne Systeme zur Unterstützung des Betriebs, MÜSSEN gehärtet sein, d.h. sie MÜSSEN so konfiguriert werden, dass die für den Betrieb der CAs nicht benötigten Accounts, Dienste, Protokolle und Ports deaktiviert werden.

Die Systeme MÜSSEN mit einem Integritätsschutz versehen sein, der vor Viren, Schadcode und dem Einspielen unerlaubter Software schützt.

Die Systeme MÜSSEN so dimensioniert sein, dass sie hinreichend performant sind und einen ununterbrochenen Betrieb gewährleisten.

Die zur Zertifikatserzeugung und ggf. -sperrung erfassten Daten inkl. der Protokolldaten gemäß Kap. 5.4.1 MÜSSEN so gesichert werden, dass deren Integrität, Vertraulichkeit und Verfügbarkeit über den gesamten Aufbewahrungszeitraum sichergestellt sind.

[TLS] [SMIME] Die Accounts der zugriffsberechtigten Personen MÜSSEN mindestens alle drei Monate überprüft werden, nicht mehr benötigte Accounts MÜSSEN deaktiviert werden.

Bei allen Systemen, die eine Multi-Faktor-Authentisierung unterstützen, MUSS eine Multi-Faktor-Authentisierung umgesetzt werden.

Die Authentifizierungsschlüssel und Passworte der privilegierten Accounts der CA-Systeme MÜSSEN geändert werden, wenn sich die Berechtigung einer Person zum administrativen Zugriff auf die Systeme ändert oder entzogen wird.

Für vertrauenswürdige Rollen MUSS sichergestellt werden, dass sich diese zur Nachvollziehbarkeit mit persönlichen Accounts an den Systemen anmelden.

Für vertrauenswürdige Rollen, die sich mittels Benutzername und Passwort an den Systemen anmelden, MÜSSEN, sofern technisch möglich, die nachfolgend aufgeführten Maßnahmen umgesetzt werden:

- Für Accounts, auf die nur in sicheren Umgebungen zugegriffen werden kann, MÜSSEN Passwörter mit mindestens 12 Zeichen Länge gefordert werden.
- Für Accounts, auf die von außerhalb einer Sicherheitszone zugegriffen werden kann, MÜSSEN Kennwörter mit mindestens acht Zeichen gefordert werden, bei denen es sich nicht um eines der vorherigen vier Kennwörter des Benutzers handelt und es MUSS eine Kontosperre nach fünf fehlgeschlagenen Zugriffsversuchen (s.u.) umgesetzt werden.
- Bei der Entwicklung von Passwort-Richtlinien SOLLTEN die Passwort-Richtlinien in NIST 800-63B Anhang A berücksichtigt werden.
- wenn ein TSP eine Passwortrichtlinie hat, welche eine routinemäßige periodische Passwortänderungen erfordert, DARF dieser Zeitraum NICHT weniger als zwei Jahre betragen.

Personen in vertrauenswürdigen Rollen MÜSSEN verpflichtet werden, sich von ihrem Account abzumelden oder ihren Arbeitsplatz zu sperren, wenn sie nicht mehr in der Rolle tätig sind.

Die Arbeitsplätze MÜSSEN entweder so konfiguriert werden, dass diese automatisch nach einer festgelegten Zeit der Inaktivität des Nutzers gesperrt werden oder die relevanten Anwendungen MÜSSEN so konfigurieren, dass diese automatisch nach einer festgelegten Zeit der Inaktivität des Nutzers zur Abmeldung des Accounts führen.

Der Zugang zu CA-Systemen MUSS nach fünf fehlgeschlagenen Anmeldeversuchen gesperrt werden, vorausgesetzt, dass das CA-System diese Maßnahme unterstützt, die Maßnahme nicht für Denial of Service-Angriffe genutzt werden kann und die Maßnahme nicht die Sicherheit dieser Authentifizierungskontrolle schwächt.

Für den administrativen Zugriff auf kritische Systeme MUSS eine Multi-Faktor-Authentisierung oder eine Mehr-Personen-Authentifizierung sichergestellt werden.

Für alle Accounts der vertrauenswürdigen Rollen an den CA-Systemen, die von außerhalb der sicheren Umgebungen erreichbar sind, MUSS eine Multifaktor-Authentisierung sichergestellt werden.

Remote-Zugriffe auf kritische Systeme DÜRFEN nur dann zugelassen werden, wenn diese von Systemen ausgehen, die dem TSP gehören oder vom TSP kontrolliert werden und die temporär über einen verschlüsselten Kanal auf Basis einer Multifaktor-Authentisierung gegenüber einem gesicherten System im Netzwerk des TSP aufgebaut werden, welches die Verbindung zu den kritischen Systemen vermittelt.

6.5.2 Sicherheitsbewertung von Computern

Keine Vorgabe.

6.6 Technische Kontrollen des Lebenszyklus

6.6.1 Steuerung der Systementwicklung

Bereits in der Entwurfs- und Anforderungsspezifikationsphase eines Systementwicklungsprojekts MUSS eine Analyse der Sicherheitsanforderungen durchgeführt werden, um sicherzustellen, dass die Sicherheit der Systeme von vorneherein berücksichtigt wird.

Für Produktion, Test und Entwicklung MÜSSEN getrennte Systeme verwendet werden.

6.6.2 Maßnahmen des Sicherheitsmanagements

Alle Releases, Patches und kurzfristigen Bugfixes sowie Änderungen der Konfiguration, welche die Sicherheitsrichtlinien betreffen, MÜSSEN über geregelte Changemanagement-Prozesse abgewickelt und dokumentiert werden.

Alle Änderungen, die sich auf das vom TSP festgelegte Sicherheitsniveau auswirken, MÜSSEN vom Management und ggf. vom ISMS freigegeben werden.

Es MUSS sichergestellt werden, dass

- Sicherheitspatches in einer angemessenen Zeit, spätestens jedoch innerhalb von 6 Monaten, eingespielt werden,
- Sicherheitspatches nicht eingespielt werden, wenn diese zusätzliche Schwachstellen oder Instabilitäten mit sich bringen, welche den Vorteil des Patches überwiegen,
- die Gründe für das Nicht-Einspielen von Sicherheitspatches dokumentiert werden.

Folgende Aktivitäten MÜSSEN kontinuierlich überwacht werden und es MÜSSEN geeignete Alarmierungsfunktionen implementiert werden:

- Sicherheitsrelevante Systemereignisse gemäß Kap. 5.4.1
- Verfügbarkeit und Nutzung der benötigten Dienste
- Konfigurationsänderungen, die nicht auf Basis eines autorisierten Changes durchgeführt wurden

Bei der Überwachung SOLLTE die Sensibilität aller gesammelten oder analysierten Informationen berücksichtigt werden.

Die TSP SOLLTEN die Datensicherungen regelmäßig testen, um sicherzustellen, dass diese den Anforderungen des Notfallplans genügen. Die Datensicherungs- und Rücksicherungsfunktionen MÜSSEN von dafür vorgesehen vertrauenswürdigen Rollen durchgeführt werden.

[TLS] [SMIME] Ergänzend zu den vorgenannten Ereignissen MÜSSEN folgende Aktivitäten überwacht werden:

- Änderungen von Sicherheitsprofilen
- Installation, Aktualisierung und Entfernung von Software auf einem Zertifikatssystem
- Systemabstürze, Hardware-Ausfälle und andere Anomalien
- Firewall und Router-Aktivitäten
- Zu- und Austritte in und aus den Betriebsräumen der Zertifikatsmanagementsysteme

[NCP] Der Kapazitätsbedarf der Systeme MUSS überwacht werden und Prognosen für den zukünftigen Kapazitätsbedarf MÜSSEN erstellt werden, um sicherzustellen, dass angemessene Verarbeitungsleistungen und Speicherkapazitäten zur Verfügung stehen.

6.6.3 Sicherheitskontrollen während des Lebenszyklus

Keine Vorgabe.

6.7 Netzwerk-Sicherheitskontrollen

Die internen Netze und Systeme MÜSSEN vor unautorisierten Zugriffen und Angriffen geschützt werden, z.B. durch Firewalls. Die Netzwerkkomponenten (bspw. Firewalls, Router) MÜSSEN so konfiguriert werden, dass alle nicht benötigten Protokolle und Zugänge deaktiviert sind.

Die Netzwerke oder Zonen MÜSSEN auf der Grundlage einer Risikobewertung unter Berücksichtigung der funktionalen, logischen und physischen (einschließlich Standort) Beziehung zwischen vertrauenswürdigen Systemen und Diensten segmentiert werden.

Alle für den Betrieb der TSP kritischen Systeme MÜSSEN in sicheren oder hochsicheren Zonen untergebracht werden. Die Root-CA-Systeme MÜSSEN in hochsicheren Zonen untergebracht werden und offline bzw. von allen anderen Netzen getrennt betrieben werden. Es MÜSSEN Sicherheitsverfahren implementiert und konfiguriert werden, welche die Systeme und die Kommunikation zwischen Systemen innerhalb von Sicherheitszonen schützt.

Lokale Netzwerkkomponenten (z.B. Router) MÜSSEN in physikalisch und logisch sicheren Umgebungen installiert sein. Deren Konfigurationen MÜSSEN regelmäßig auf Übereinstimmung mit den vom TSP definierten Anforderungen geprüft werden.

Die Netzwerke zur Administration der Systeme MÜSSEN von den operativen Netzwerken separiert werden.

Innerhalb einer Zone MÜSSEN für alle Systeme die gleichen Sicherheitsanforderungen gelten.

Zwischen den Zonen MÜSSEN Sicherheitssysteme implementiert werden, welche die Systeme und Kommunikation innerhalb der sicheren Zonen sowie die Kommunikation mit den Systemen außerhalb der Zonen schützen. Die Verbindungen MÜSSEN so eingeschränkt werden, dass nur die zum Betrieb erforderlichen Verbindungen möglich sind, nicht benötigte Verbindungen MÜSSEN explizit verboten oder deaktiviert werden. Alle Netzwerkgeräte an den Zonengrenzen (Firewalls, Router, Switches, Gateways oder sonstige Geräte) MÜSSEN so konfiguriert werden, dass ausschließlich die Dienste, Protokolle, Ports und Kommunikationsbeziehungen zugelassen werden, die für den Betrieb der CAs erforderlich sind. Diese Regeln MÜSSEN regelmäßig überprüft werden.

Für die Kommunikation zwischen verschiedenen vertrauenswürdigen Systemen MÜSSEN vertrauenswürdige Kanäle genutzt werden, die sich logisch von anderen Kommunikationskanälen unterscheiden und eine sichere Identifizierung ihrer Endpunkte sowie die Integrität und Vertraulichkeit der übertragenen Daten gewährleisten.

Sofern eine hohe Verfügbarkeit des externen Zugriffs gefordert ist, MÜSSEN die externen Netzwerkverbindungen redundant aufgebaut sein.

Schwachstellenprüfungen an öffentlichen und privaten IP-Adressen, die vom TSP identifiziert wurden, MÜSSEN mindestens quartalsweise durchgeführt werden. Die Schwachstellenprüfungen MÜSSEN von Personen oder Organisationen durchgeführt werden, die über die für einen zuverlässigen Bericht erforderlichen Fähigkeiten, Werkzeuge, Fertigkeiten, ethischen Grundsätze und Unabhängigkeit verfügen. Die Durchführung der Schwachstellenprüfung MUSS mit Angabe der Qualifikation der prüfenden Person oder Organisation dokumentiert werden.

Bei Inbetriebnahme oder bei signifikanten Änderungen an der Infrastruktur oder den Anwendungen, mindestens aber einmal pro Jahr MÜSSEN die Systeme Penetrationstests unterzogen werden. Die Penetrationstests MÜSSEN von Personen oder Organisationen durchgeführt werden, die über die für einen zuverlässigen Bericht erforderlichen Fähigkeiten, Werkzeuge, Fertigkeiten, ethischen Grundsätze und Unabhängigkeit verfügen. Die Durchführung der Penetrationstests MUSS mit Angabe der Qualifikation der prüfenden Person oder Organisation dokumentiert werden.

Innerhalb von 48 Stunden nach der Entdeckung einer kritischen Schwachstelle

- MUSS diese Schwachstelle behoben werden oder
- wenn eine Behebung der Schwachstelle innerhalb von 48 Stunden nicht möglich ist, MUSS ein Plan zur Minderung der Schwachstelle, inkl. einer Priorisierung anhand der betroffenen Systeme, erstellt werden oder
- die faktische Grundlage für die Entscheidung des TSP, dass eine Schwachstelle nicht behoben werden muss, weil entweder der TSP mit der Einstufung nicht einverstanden ist oder es sich nicht um eine Schwachstelle handelt („False Positive“) oder die Ausnutzung der Schwachstelle durch kompensierende Kontrollen oder das Fehlen von Bedrohungen verhindert wird oder andere ähnliche Gründe vorliegen, MUSS dokumentiert werden.

[TLS] [SMIME] Es MÜSSEN Intrusion-Detection- (IDS) und Intrusion-Prevention-Systeme (IPS) implementiert werden, welche die TSP selbst unter Kontrolle haben oder an vertrauenswürdige Dritte delegiert haben.

Die o.g. Schwachstellenprüfungen MÜSSEN

- innerhalb einer Woche auf Anfrage des CA/Browser-Forums und
- bei signifikanten Änderungen an der Infrastruktur oder den Anwendungen

durchgeführt werden.

[3145] Wenn ein IDS verwendet wird, MÜSSEN die vom IDS aufgezeichneten Protokolldateien bei jedem Vorfall sowie regelmäßig in einem vom TSP festgelegten Zeitraum ausgewertet werden.

[VS-NfD] Bei der Netzwerktrennung MUSS [ISI LANA] als Leitfaden angewendet werden.

6.8 Zeitstempel

Alle Systeme MÜSSEN regelmäßig, mindestens jedoch täglich über einen Zeitserver mittels Network Time Protocol (NTP) mit exakten Zeitinformationen (UTC) synchronisiert werden, so dass die Zeitstempel in Logs und Aufzeichnungen verlässlich sind.

7 ZERTIFIKATS-, SPERRLISTEN- UND OCSP-PROFILE

7.1 Zertifikatsprofile

Die Zertifikatsprofile MÜSSEN [RFC5280] und [X.509] entsprechen und in den CPS beschrieben werden.

Die Zertifikatsprofile gelten für alle Zertifikate, die ab dem Gültigkeitsbeginn dieser CP ausgestellt werden. Bereits ausgestellte Zertifikate mit Profilen gemäß älterer Anforderungen behalten ihre Gültigkeit bei, sofern nicht explizit auf deren Ungültigkeit hingewiesen wird.

Der Gültigkeitsbeginn eines Zertifikats DARF NICHT vor dessen Ausstellungszeitpunkt liegen, er DARF jedoch ggf. auf einen späteren Zeitpunkt gesetzt werden.

Die Seriennummern der Zertifikate MÜSSEN mit einem kryptographisch sicheren Zufallszahlengenerator erzeugt werden.

[TLS] [SMIME] Seriennummern MÜSSEN eine Entropie von mindestens 64 Bit aufweisen.

[TLS] Pre-Zertifikate gemäß [RFC6962] (“Certificate Transparency”) gelten nicht als gültige Zertifikate im Sinne des [RFC5280]. Mit der Ausstellung eines Pre-Zertifikates erklärt der TSP verbindlich, das korrespondierende Leaf-Zertifikat auszustellen. HINWEIS: Telekom Security stellt Pre-Zertifikate ausschließlich von derselben CA aus, welche auch später die Leaf-Zertifikate ausstellt.

Anmerkung: Nachfolgend werden die zu verwendenden Erweiterungen, OIDs und Namensbestandteile beschrieben. Der besseren Übersichtlichkeit halber sind die Zertifikatsprofile einzelner Zertifikatstypen in Anhang D zusammenfassend dargestellt.

7.1.1 Versionsnummer

Alle X509-Zertifikate MÜSSEN in der Version 3 ausgestellt werden.

7.1.2 Zertifikatserweiterungen

Tabelle 2 gibt einen Überblick über die nutzbaren Zertifikatserweiterungen. Erweiterungen, die dort nicht aufgeführt sind, DÜRFEN grundsätzlich NICHT verwendet werden, Ausnahmen MÜSSEN in den CPS beschrieben werden.

Für die in Tabelle 2 aufgeführten Erweiterungen gelten folgende Anforderungen bzgl. der Kritikalität:

- `keyUsage` MUSS in allen Zertifikaten als kritisch markiert werden.
- `basicConstraints` MUSS in CA-Zertifikaten als kritisch markiert werden, in allen anderen Zertifikaten DARF sie als kritisch markiert werden.
- Alle anderen Erweiterungen DÜRFEN NICHT als kritisch markiert werden.

Wenn es für Erweiterungen über den Standard hinausgehende Anforderungen gibt, so sind diese der Tabelle nachfolgend aufgeführt und in der Spalte Anforderungen referenziert.

Tabelle 2 - Zertifikatserweiterungen

Erweiterung	OID	Anforderungen
authorityKeyIdentifier	2.5.29.35	(01)
subjectKeyIdentifier	2.5.29.14	(01)
keyUsage	2.5.29.15	(02)-(07)
certificatePolicies	2.5.29.32	(08)-(17)
subjectAltName	2.5.29.17	(18)-(20)
basicConstraints	2.5.29.19	(21)-(22)
extendedKeyUsage	2.5.29.37	(23)-(30)
cRLDistributionPoints	2.5.29.31	(31)-(33)
authorityInfoAccess	1.3.6.1.5.5.7.1.1	(34)-(36)
qcStatements	1.3.6.1.5.5.7.1.3	(37)-(38)
validityModel	1.3.6.1.4.1.8301.3.5	-
id-pkix-ocsp-nocheck	1.3.6.1.5.5.7.48.1.5	Siehe Kap. 7.3
cabfOrganizationIdentifier	2.23.140.3.1	(39)
signedCertificateTimestampList	1.3.6.1.4.1.11129.2.4.2	(40)
id-etsi-ext-valassured-ST-certs	0.4.0.194121.2.1	(41)
precertificate poison extension	1.3.6.1.4.1.11129.2.4.3	(42)

authorityKeyIdentifier, subjectKeyIdentifier

(01) Wenn der authorityKeyIdentifier gesetzt wird, MUSS der keyIdentifier gemäß [RFC5280#4.2.1.1] gesetzt werden und dem subjectKeyIdentifier der ausstellenden CA entsprechen.

keyUsage

(02) In CA-Zertifikaten MÜSSEN keyCertSign oder cRLSign gesetzt werden. digitalSignature MUSS gesetzt werden, wenn mit dem Zertifikat auch OCSP-Antworten signiert werden, ansonsten DARF es gesetzt werden. Andere Werte DÜRFEN NICHT gesetzt werden.

(03) In Endteilnehmer-Zertifikaten DÜRFEN keyCertSign und cRLSign NICHT gesetzt werden. Die Werte MÜSSEN ihrem Anwendungszweck entsprechend gesetzt werden, siehe [RFC5280#4.2.1.3]. Wenn auch die extendedKeyUsage gesetzt wird, MUSS die keyUsage konsistent zur extendedKeyUsage gesetzt werden (siehe [RFC5280#4.2.1.12]).

(04) In OCSP-Signer-Zertifikaten MUSS digitalSignature gesetzt werden, weitere Werte DÜRFEN NICHT gesetzt werden.

(05) [ETSI] In Endteilnehmer-Zertifikaten für natürliche Personen oder Organisationen MUSS eine der folgenden Varianten der `keyUsage` gesetzt werden:
a) `nonRepudiation`
b) `nonRepudiation` und `digitalSignature`
c) `digitalSignature`
d) `digitalSignature` und [`keyEncipherment` oder `keyAgreement`]
e) `keyEncipherment` oder `keyAgreement`
f) `nonRepudiation` und `digitalSignature` und [`keyEncipherment` oder `keyAgreement`]
Um eine gemischte Verwendung von Schlüsseln zu vermeiden, SOLLTEN nur die Varianten a), c) oder e) genutzt werden.
In Zertifikaten, mit denen die Verpflichtung zu signierten Inhalten bestätigt wird, MUSS eine der Varianten a), b) oder f) genutzt werden, davon SOLLTE Variante a) genutzt werden.

(06) [SMIME] In Endteilnehmer-Zertifikaten MUSS die `keyUsage` gemäß dem Anwendungszweck eine der unter (05) aufgeführten Varianten b), c), d), e) oder f) gesetzt werden,

(07) [TLS] In Endteilnehmer-Zertifikaten MUSS die `keyUsage` gemäß dem Anwendungszweck eine der unter (05) aufgeführten Varianten c) oder d) gesetzt werden, davon SOLLTE Variante c) genutzt werden.

`certificatePolicies`

(08) Es SOLLTEN grundsätzlich nur OIDs verwendet werden. Wenn die alleinige Nutzung von OIDs unzureichend ist, DÜRFEN zusätzlich `cPSuri` mit einer gültigen http- oder https-URL oder `userNotice` gesetzt werden. OIDs DÜRFEN NICHT mehrfach gesetzt werden.

(09) [TLS] In Sub-CA-Zertifikaten MUSS entweder `anyPolicy` oder die anwendbare OID gemäß [BR] enthalten sein.
Wenn die anwendbare OID gemäß [BR] gesetzt wird, gelten folgende Anforderungen:
- Es DÜRFEN NICHT mehrere OIDs gemäß [BR] gesetzt werden.
- Darüber hinaus DÜRFEN weitere OIDs gemäß [ETSI] sowie OIDs des TSP, die in dem relevanten CPS beschrieben sind, gesetzt werden.

(10) [SMIME] In Sub-CA-Zertifikaten MUSS entweder `anyPolicy` oder die anwendbare(n) OID(s) gemäß [SBR] enthalten sein. Wenn anwendbare OIDs gemäß [SBR] gesetzt sind, DÜRFEN weitere OIDs gemäß [ETSI] sowie OIDs des TSP, die in dem relevanten CPS beschrieben sind, gesetzt werden.

(11) [SMIME] Wenn in Sub-CA- oder Endteilnehmer-Zertifikaten eine `userNotice` gesetzt wird, MUSS diese `explicitText` enthalten und DARF NICHT `noticeRef` enthalten.

(12) [TLS] [SMIME] Die in Sub-CA- und Endteilnehmer-Zertifikaten gesetzten `certificatePolicies` MÜSSEN zueinander korrespondieren, d.h. es DÜRFEN von einer Sub-CA NICHT Endteilnehmer-Zertifikate mit OIDs ausgestellt werden, welche in dem Sub-CA-Zertifikat selbst nicht enthalten sind, sofern im Sub-CA Zertifikat nicht `anyPolicy` gesetzt ist („Policy-Verkettung“).

(13) [ETSI] In Endteilnehmer-Zertifikaten für natürliche Personen oder Organisationen MUSS mindestens eine OID gesetzt sein. Es SOLLTEN die von ETSI reservierten OIDs verwendet werden:
- [NCP] `0.4.0.2042.1.1`
- [NCP+] `0.4.0.2042.1.2`
- [LCP] `0.4.0.2042.1.3`
- [QCP-n] `0.4.0.194112.1.0`
- [QCP-l] `0.4.0.194112.1.1`
- [QCP-n-qscd] `0.4.0.194112.1.2`
- [QCP-l-qscd] `0.4.0.194112.1.3`

Die OID für `2.5.29.32.0 (anyPolicy)` DARF NICHT gesetzt werden.

(14) [TLS] In Endteilnehmer-Zertifikaten MUSS die korrespondierende OID gemäß [BR] gesetzt sein:
- [EVCP] `2.23.140.1.1`
- [DVCP] `2.23.140.1.2.1`
- [OVCP] `2.23.140.1.2.2`

Bei qualifizierten Website-Zertifikaten SOLLTE zusätzlich die korrespondierende ETSI-OID gesetzt sein:
- [QEVCP-w] `0.4.0.194112.1.4`
- [QNCP-w] `0.4.0.194112.1.5`

Darüber hinaus DÜRFEN eigene OIDs des TSP, die in dem relevanten CPS des TSP beschrieben sind, und/oder nachfolgende von ETSI reservierte OIDs verwendet werden:
- [EVCP] `0.4.0.2042.1.4`
- [DVCP] `0.4.0.2042.1.6`
- [OVCP] `0.4.0.2042.1.7`

Des Weiteren DARF `cPSuri` mit einem Verweis (http URL) zum CPS oder anderen online verfügbaren Informationen des TSP gesetzt werden. `userNotice` DARF NICHT gesetzt werden.

(15) [EVCP] In Endteilnehmer-Zertifikaten MUSS `cPSuri` mit einem Verweis (http URL) zum CPS gesetzt werden.

(16) [SMIME] In Endteilnehmer-Zertifikaten MUSS mindestens die korrespondierende OID gemäß [SBR] gesetzt sein:

- [SMV]
  - [Legacy] `2.23.140.1.5.1.1`
  - [Multipurpose] `2.23.140.1.5.1.2`
  - [Strict] `2.23.140.1.5.1.3`
- [SOV]
  - [Legacy] `2.23.140.1.5.2.1`
  - [Multipurpose] `2.23.140.1.5.2.2`
  - [Strict] `2.23.140.1.5.2.3`
- [SSV]
  - [Legacy] `2.23.140.1.5.3.1`
  - [Multipurpose] `2.23.140.1.5.3.2`
  - [Strict] `2.23.140.1.5.3.3`
- [SIV]
  - [Legacy] `2.23.140.1.5.4.1`
  - [Multipurpose] `2.23.140.1.5.4.2`
  - [Strict] `2.23.140.1.5.4.3`

Darüber hinaus DÜRFEN eigene OIDs des TSP, die in dem relevanten CPS beschrieben sind, und/oder die von ETSI reservierten OIDs (siehe (13)) verwendet werden.

(17) [3145] In Endteilnehmer-Zertifikaten DARF `cPSuri` mit einem Verweis (http URL) zum CPS gesetzt werden. `userNotice` DARF NICHT gesetzt werden.

`subjectAltName`

(18) Der `subjectAltName` DARF in den Zertifikaten aller Hierarchieebenen gesetzt werden. Alle prüfbaren Inhalte MÜSSEN geprüft werden.

(19) [TLS] `subjectAltName` DARF in CA-Zertifikaten NICHT gesetzt werden.
In Endteilnehmer-Zertifikaten MUSS mindestens ein Eintrag im `subjectAltName` aufgenommen werden.
Zulässige Angaben sind FQDNs oder Wildcard Domain Names als `dNSName` oder IPv4- oder IPv6-Adressen als `iPAddress`.
Die FQDNs sowie die FQDN-Anteile von Wildcard Domain Names MÜSSEN ausschließlich aus „P-Labels“ oder „Non-Reserved LDH-Labels“ bestehen. Reservierte IP-Adressen oder interne Namen (gemäß Anhang C) DÜRFEN NICHT eingetragen werden.

(20) [SMIME] In Endteilnehmer-Zertifikaten MUSS mindestens eine E-Mail-Adresse als `rFC822Name` oder `otherName` (`id-on-SmtpUTF8Mailbox`) gemäß [SBR] im `subjectAltName` aufgenommen werden.

basicConstraints

(21) In CA-Zertifikaten MUSS `cA` auf `true` gesetzt sein.
In Sub-CA-Zertifikaten SOLLTE eine maximale Pfadlänge in `pathLenConstraint` angegeben werden, in Root-CA-Zertifikaten SOLLTE diese Angabe NICHT gemacht werden.

(22) In Endteilnehmer- und OCSP-Signer-Zertifikaten MUSS `cA` auf `false` gesetzt sein, `pathLenConstraint` DARF NICHT gesetzt werden.

extendedKeyUsage

(23) Wenn die `extendedKeyUsage` gesetzt ist, MUSS diese gemäß [RFC5280#4.2.1.12] konsistent zur `keyUsage` sein.

(24) [TLS] In Sub-CA-Zertifikaten[7] MUSS `id-kp-serverAuth` eingetragen werden. Es DARF darüber hinaus `id-kp-clientAuth` eingetragen werden. `id-kp-emailProtection`, `id-kp-codeSigning`, `id-kp-timeStamping`, `id-kp-OCSPSigning` und `anyExtendedKeyUsage` DÜRFEN NICHT aufgenommen werden. Andere Werte SOLLTEN NICHT aufgenommen werden.

(25) [SMIME] In Sub-CA-Zertifikaten[7] MUSS `id-kp-emailProtection` eingetragen werden. Es DÜRFEN weitere Werte eingetragen werden, jedoch DÜRFEN `anyExtendedKeyUsage`, `id-kp-codeSigning`, `id-kp-timeStamping` und `id-kp-serverAuth` NICHT aufgenommen werden.

(26) In Sub-CA-Zertifikaten unterhalb der öffentlichen Telekom Roots, die nicht zur Ausstellung von TLS-Server-Zertifikaten verwendet werden, DARF `id-kp-serverAuth` NICHT gesetzt werden.

(27) [TLS] [SMIME] Die in Sub-CA- und Endteilnehmer-Zertifikaten gesetzten `extendedKeyUsage` MÜSSEN zueinander korrespondieren, d.h. es DÜRFEN von einer Sub-CA NICHT Endteilnehmer-Zertifikate mit Werten ausgestellt werden, welche in dem Sub-CA-Zertifikat selbst nicht enthalten sind („EKU-Verkettung“).
Hiervon ausgenommen sind OCSP-Signer-Zertifikate, die auch von Sub-CAs ausgestellt werden DÜRFEN, welche selbst nicht `id-kp-OCSPSigning` enthalten.

(28) [TLS] In Endteilnehmer-Zertifikaten MUSS `id-kp-serverAuth` eingetragen werden. Darüber hinaus DARF auch `id-kp-clientAuth` eingetragen werden. Weitere Werte DÜRFEN NICHT eingetragen werden

[7] Diese Anforderung gilt nicht für Cross-Zertifikate.

(29) [SMIME] In Endteilnehmer-Zertifikaten MUSS `id-kp-emailProtection` eingetragen werden.
[Legacy] [Multipurpose] Darüber hinaus DÜRFEN weitere Werte eingetragen werden, jedoch DÜRFEN `anyExtendedKeyUsage`, `id-kp-codeSigning`, `id-kp-timeStamping` und `id-kp-serverAuth` NICHT eingetragen werden.
[Strict] Weitere Werte DÜRFEN NICHT eingetragen werden.

(30) In OCSP-Signer-Zertifikaten MUSS `id-kp-OCSPSigning` eingetragen werden. Weitere Werte DÜRFEN NICHT eingetragen werden.

`cRLDistributionPoints`

(31) In allen Zertifikaten, welche per CRL prüfbar sind, MÜSSEN `cRLDistribution-Points` gesetzt werden.

(32) [TLS] [SMIME] In Sub-CA- und Endteilnehmer-Zertifikaten MÜSSEN `cRLDistributionPoints` mindestens eine http-URL in `distributionPoints` enthalten.
`Reasons` und `CRLIssuer` DÜRFEN NICHT gesetzt werden
[Legacy] Es DÜRFEN weitere Verteilpunkte, z.B. per LDAP, aufgenommen werden.

(33) [3145] [ETSI] In Endteilnehmer-Zertifikaten MÜSSEN `cRLDistributionPoints` mindestens eine öffentlich erreichbare http- oder ldap-URL in `distributionPoints` enthalten.

`authorityInfoAccess`

(34) In allen Zertifikaten, welche per OCSP prüfbar sind, MUSS `authorityInfoAccess` gesetzt werden und MUSS mindestens die http-URL des OCSP-Responders in `id-ad-ocsp` enthalten.

(35) [TLS] [SMIME] In Sub-CA- und Endteilnehmer-Zertifikaten SOLLTE zusätzlich die http-URL zum Abruf des ausstellenden CA-Zertifikats in `caIssuers` enthalten sein.

(36) [ETSI] In Endteilnehmer-Zertifikaten MUSS `authorityInfoAccess` gesetzt werden und MUSS mindestens eine http(s)-URL zum Abruf des ausstellenden CA-Zertifikats in `caIssuers` enthalten.

qcStatements

(37) [QCP] In Endteilnehmer-Zertifikaten MÜSSEN folgende qcStatements gesetzt werden:
- qcs-QcCompliance (0.4.0.1862.1.1)
- qcs-QcPDS (0.4.0.1862.1.5)
- qcs-QcType (0.4.0.1862.1.6) mit einem der folgenden Werte:
  - qct-esign (0.4.0.1862.1.6.1)
  - qct-eseal (0.4.0.1862.1.6.2)
  - qct-web (0.4.0.1862.1.6.3)

Darüber hinaus DÜRFEN folgende qcStatements gesetzt werden:
- qcs-QcLimitValue (0.4.0.1862.1.2)
- qcs-QcRetentionPeriod (0.4.0.1862.1.3)

qcs-qcCClegislation (0.4.0.1862.1.7) DARF NICHT gesetzt werden.

Bzgl. der zu verwendenden Syntax MUSS [ETS4125] berücksichtigt werden.

(38) [QCP-n-qscd] [QCP-l-qscd] In Endteilnehmer-Zertifikaten MUSS qcs-QcSSCD (0.4.0.1862.1.4) gesetzt werden.

cabfOrganizationIdentifier

(39) [EVCP] Wenn der cabfOrganizationIdentifier gesetzt wird, MUSS dieser mit dem gleichen Wert wie der organizationIdentifier gesetzt werden.

signedCertificateTimestampList

(40) [TLS] In Endteilnehmer-Zertifikaten MÜSSEN mindestens drei SCT von zwei unterschiedlichen CTLog-Betreibern im Status usable enthalten sein.

id-etsi-ext-valassured-ST-certs

(41) In Kurzzeitzertifikaten, welche nicht gesperrt werden können, MUSS die Erweiterung id-etsi-ext-valassured-ST-certs gesetzt werden.
In Kurzzeitzertifikaten, welche gesperrt werden können, SOLLTE die Erweiterung id-etsi-ext-valassured-ST-certs NICHT gesetzt werden.
In Endteilnehmer-Zertifikaten, die keine Kurzzeitzertifikate sind, DARF die Erweiterung id-etsi-ext-valassured-ST-certs NICHT gesetzt werden.

precertificate poison extension

(42) [TLS] In Pre-Zertifikaten MUSS die Erweiterung precertificate poison extension gemäß [RFC6962] gesetzt werden, in allen anderen Zertifikaten DARF sie NICHT gesetzt werden.

7.1.3 Algorithmen-OID

Die für die Signatur der Zertifikate aller Hierarchieebenen verwendeten Algorithmen MÜSSEN den Anforderungen aus [SOGIS] genügen.

CA-Zertifikate, die auf einem RSA-Schlüssel basieren, MÜSSEN zur Signatur der von ihnen ausgestellten Zertifikate einen der folgenden Signaturalgorithmen verwenden:

- `sha256WithRSAEncryption (1.2.840.113549.1.1.11)`, der Hex-codierte Wert des `AlgorithmIdentifier` MUSS folgendem Wert entsprechen: `300d06092a864886f70d01010b0500`
- `sha384WithRSAEncryption (1.2.840.113549.1.1.12)`, der Hex-codierte Wert des `AlgorithmIdentifier` MUSS folgendem Wert entsprechen: `300d06092a864886f70d01010c0500`
- `sha512WithRSAEncryption (1.2.840.113549.1.1.13)`, der Hex-codierte Wert des `AlgorithmIdentifier` MUSS folgendem Wert entsprechen: `300d06092a864886f70d01010d0500`
- `rsassa-pss(1.2.840.113549.1.1.10)`
  - MGF-1 with SHA-256, and a salt length of 32 bytes, der Hex-codierte Wert des `AlgorithmIdentifier` MUSS folgendem Wert entsprechen: `304106092a864886f70d01010a3034a00f300d060960864801650304020105050a11c301a06092a864886f70d010108300d060960864801650304020105 00a203020120`
  - MGF-1 with SHA-384, and a salt length of 48 bytes, der Hex-codierte Wert des `AlgorithmIdentifier` MUSS folgendem Wert entsprechen: `304106092a864886f70d01010a3034a00f300d060960864801650304020205050a11c301a06092a864886f70d010108300d060960864801650304020205 00a203020130`
  - MGF-1 with SHA-512, and a salt length of 64 bytes, der Hex-codierte Wert des `AlgorithmIdentifier` MUSS folgendem Wert entsprechen: `304106092a864886f70d01010a3034a00f300d060960864801650304020305050a11c301a06092a864886f70d010108300d060960864801650304020305 00a203020140`

CA-Zertifikate, die auf einem P256-ECDSA-Schlüssel basieren, MÜSSEN zur Signatur der von ihnen ausgestellten Zertifikate den Signaturalgorithmus `ecdsa-with-SHA256 (1.2.840.10045.4.3.2)` verwenden. Der Hex-codierte Wert des `AlgorithmIdentifier` MUSS folgendem Wert entsprechen: `300a06082a8648ce3d040302`.

CA-Zertifikate, die auf einem P384-ECDSA-Schlüssel basieren, MÜSSEN zur Signatur der von ihnen ausgestellten Zertifikate den Signaturalgorithmus `ecdsa-with-SHA384 (1.2.840.10045.4.3.3)` verwenden. Der Hex-codierte Wert des `AlgorithmIdentifier` MUSS folgendem Wert entsprechen: `300a06082a8648ce3d040303`

Zertifikate, die auf RSA-Schlüsseln basieren, MÜSSEN `rsaEncryption (1.2.840.113549.1.1.1)` mit `NULL` Parameter in der `subjectPublicKeyInfo` enthalten. Der Hex-codierte Wert des `AlgorithmIdentifier` MUSS folgendem Wert entsprechen: `300d06092a864886f70d0101010500`

Zertifikate, die auf EC-Schlüsseln basieren, MÜSSEN `ecPublicKey (1.2.840.10045.2.1)` ohne `NULL` Parameter und zusätzlich, in Abhängigkeit der verwendeten Kurve, einer der folgenden Werte in der `subjectPublicKeyInfo` enthalten:

- P256: `prime256v1 (1.2.840.10045.3.1.7)`, der Hex-codierte Wert des `AlgorithmIdentifier` MUSS folgendem Wert entsprechen: `301306072a8648ce3d020106082a8648ce3d030107`
- P384: `secp384r1 (1.3.132.0.34)`, der Hex-codierte Wert des `AlgorithmIdentifier` MUSS folgendem Wert entsprechen: `301006072a8648ce3d020106052b81040022`

Die verwendeten Algorithmen und Parameter MÜSSEN in den CPS aufgeführt werden.

7.1.4 Namensformen

Grundsätzliches:

- Der `issuerDN` eines Zertifikats MUSS dem `subjectDN` des ausstellenden Zertifikats „Byte-für-Byte“ entsprechen.
- In CA-Zertifikaten DÜRFEN alle Attribute des `subjectDN` NICHT mehr als einmal gesetzt werden.
- In Endteilnehmer-Zertifikaten DÜRFEN grundsätzlich alle Attribute des `subjectDN` NICHT mehr als einmal gesetzt werden. Erlaubte Ausnahmen MÜSSEN in den CPS beschrieben werden.
- Attribute im `subjectDN` DÜRFEN NICHT nur Metadaten wie '.', '-' oder Leerzeichen oder andere Hinweise darauf enthalten, dass der Wert nicht vorhanden, unvollständig oder nicht anwendbar ist.
- [TLS] In Endteilnehmer-Zertifikaten MÜSSEN die Attribute gemäß [BR#7.1.4.2] codiert und in der dort aufgeführten Reihenfolge gesetzt werden.

Tabelle 3 gibt einen Überblick über obligatorische und optionale Attribute des `subjectDN` für CA-, Endteilnehmer- und OCSP-Signer-Zertifikate. Dort nicht aufgeführte Attribute DÜRFEN grundsätzlich NICHT gesetzt werden, Ausnahmen MÜSSEN in den CPS beschrieben werden.

Wenn es für Attribute über den Standard hinausgehende Anforderungen gibt, so sind diese in der Tabelle nachfolgend aufgeführt und in der Spalte Anforderungen referenziert.

Tabelle 3 - Namensformen

`subjectDN` Attribut	**OID**	**Anforderungen**
`commonName`	`2.5.4.3`	(01)-(04)
`emailAddress`	`1.2.840.113549.1.9.1`	(05)
`title`	`2.5.4.12`	(06)
`serialNumber`	`2.5.4.5`	(07)-(09)
`givenName`	`2.5.4.42`	siehe Kap. 3.1.2
`surname`	`2.5.4.4`	siehe Kap. 3.1.2
`pseudonym`	`2.5.4.65`	(10)
`streetAddress`	`2.5.4.9`	(11)
`localityName`	`2.5.4.7`	(11)
`stateOrProvinceName`	`2.5.4.8`	(11)
`postalCode`	`2.5.4.17`	(11)

businessCategory	2.5.4.15	(12)
organizationalUnitName	2.5.4.11	siehe Kap. 3.1.2
organizationIdentifier	2.5.4.97	(13)-(14), siehe Kap. 3.1.2
jurisdiction.LocalityName	1.3.6.1.4.1.311.60.2.1.1	siehe Anhang D 4.1
jurisdiction.StateOrProv.Name	1.3.6.1.4.1.311.60.2.1.2	siehe Anhang D 4.1
jurisdiction.CountryName	1.3.6.1.4.1.311.60.2.1.3	siehe Anhang D 4.1
organizationName	2.5.4.10	siehe Kap. 3.1.2
countryName	2.5.4.6	(15)-(17)

commonName

(01) In CA-Zertifikaten MUSS der commonName einen über alle von der ausstellenden CA erzeugten Zertifikate hinweg eindeutigen und gebräuchlichen Namen (nicht unbedingt der vollständige registrierte Name) des TSP beinhalten und in einer für den Markt des TSP gebräuchlichen Sprache gewählt werden.

(02) In Root-CA-Zertifikaten DÜRFEN die commonName NICHT wiederverwendet werden, d.h. in Folgezertifikaten MÜSSEN andere commonName vergeben werden.

(03) [TLS] Wenn in Endteilnehmer-Zertifikaten der commonName gesetzt wird, MUSS dieser genau einen Eintrag enthalten, der auch im subjectAltName enthalten ist. Bzgl. der Codierung des commonName gilt:
- IPv4-Adressen MÜSSEN gemäß [RFC3986] codiert sein,
- IPv6-Adressen MÜSSEN gemäß [RFC5952#4] codiert sein,
- FQDN und Wildcard Domain Names MÜSSEN eine Zeichen-für-Zeichen-Kopie des dNSName aus dem subjectAltName sein.

(04) [SMIME] Wenn in Endteilnehmer-Zertifikaten der commonName gesetzt wird, DARF die Mailbox-Adresse, wie im subjectAltName angegeben, gesetzt werden.
[SOV]: Alternativ DARF der Name der Organisation wie in organization angegeben gesetzt werden.
[SSV] [SIV]: Alternativ DARF der Name der Person wie in givenName und/oder surname angegeben oder das Pseudonym gesetzt werden.
Andere Werte DÜRFEN NICHT gesetzt werden.

emailAddress

(05) [SMIME] Wenn in Endteilnehmer-Zertifikaten emailAddress gesetzt wird, MUSS sie mit einer Mailbox-Adresse, wie im subjectAltName angegeben, gesetzt werden.

title

(06) [SIV] [SSV] Wenn title gesetzt wird, MUSS dieser mit einer organisatorischen Rolle/Titel oder einer reglementierten und verifizierten Berufsbezeichnung gesetzt werden.

serialNumber

(07) [ETSI] Wenn in Zertifikaten für natürliche Personen die `serialNumber` gesetzt wird, MUSS diese die Eindeutigkeit des Namens gewährleisten.
Die `serialNumber` hat keine definierte Semantik.

(08) [SMIME] Wenn in Endteilnehmerzertifikaten die `serialNumber` gesetzt wird, MUSS sie mit einem von der CA oder RA vergebenen Identifier zur Identifizierung oder Unterscheidung des Zertifikatsnehmers gesetzt werden.

(09) [EVCP] In Endteilnehmer-Zertifikaten MUSS die `serialNumber` die juristisch zugewiesene Nummer (Gründungsnummer oder eine ähnliche Nummer) der Organisation enthalten. Wenn keine solche Nummer vergeben wurde, MUSS das Datum der Gründung in einem gängigen Datumsformat gesetzt werden.
Bei Behörden und nicht-gewerblichen Organisationen, die keine Registrierungsnummer oder Gründungsdatum nachweisen können, MUSS eine geeignete Beschreibung aufgenommen werden, um anzuzeigen, dass es sich bei der Organisation um eine Behörde bzw. eine nicht-gewerbliche Organisation handelt.

pseudonym

(10) Wenn das `pseudonym` gesetzt ist, SOLLTE der `countryName` mit dem Wert „DE“ (Land des Sitzes der CA) gesetzt werden. Bei Zertifikaten für natürliche Personen in Verbindung mit einer Organisation DARF alternativ als `countryName` das Land des Sitzes der Organisation gesetzt werden.

streetAddress, postalCode, localityName, stateOrProvinceName

(11) [TLS] [SMIME] Wenn in Endteilnehmer-Zertifikaten `streetAddress, postalCode, localityName und/oder stateOrProvinceName` gesetzt werden, MÜSSEN diese die Adresse des Geschäftssitzes des Zertifikatsnehmers enthalten.

businessCategory

(12) `businessCategory` MUSS mit dem korrekten Organisationstyp gemäß Kap. 1.3.3 gesetzt werden

organizationIdentifier

(13) Wenn der `organizationIdentifier` gesetzt wird, MUSS er eine Registrierungsnummer der Organisation nach folgendem Schema enthalten:
- drei Zeichen für das Registrierungsschema (VAT, LEI oder NTR) gefolgt von einem Doppelpunkt
- zwei Zeichen für den Ländercode
- einen Bindestrich („-“)
- Referenz, die gemäß dem identifizierten Registrierungsschema zugewiesen wurde

(14) [EVCP] LEI DARF NICHT als Registrierungsschema verwendet werden,

countryName

(15) Wenn der countryName gesetzt wird, MUSS er mit dem zweistelligen ISO 3166-1 Ländercode des Landes des Zertifikatssubjekts gesetzt werden.

(16) [ETSI] Bzgl. der zu setzenden Werte für countryName in Endteilnehmerzertifikaten in Verbindung mit dem Attribut pseudonym siehe (10) oben.

7.1.5 Namensbeschränkungen

Namensbeschränkungen DÜRFEN in den Zertifikaten aller Hierarchiestufen NICHT gesetzt werden.

7.1.6 OIDs der Erweiterung certificatePolicies

Siehe Kap. 7.1.2.

7.1.7 Verwendung der Erweiterung policyConstraints

Keine Vorgabe.

[ETSI] In Endteilnehmerzertifikaten DÜRFEN policyConstraints NICHT gesetzt werden.

7.1.8 Syntax und Semantik der policyQualifier

policyQualifier MÜSSEN konform zu [RFC5280] mit den in Kap. 7.1.2 festgelegten Inhalten gesetzt werden.

7.1.9 Verarbeitungssemantik für certificatePolicies

certificatePolicies DÜRFEN NICHT als kritisch markiert werden, so dass es im Ermessen der Zertifikatsnutzer liegt, diese auszuwerten.

7.2 Sperrlistenprofile

Alle Sperrlisten MÜSSEN den Anforderungen des [RFC5280] genügen und von der jeweiligen CA selbst signiert werden.

Für die Signatur der Sperrlisten MÜSSEN die in Kap. 7.1.3 aufgeführten Algorithmen verwendet werden.

[TLS] [SMIME] Bei den Sperrlisten MUSS es sich immer um direkte und vollständige Sperrlisten handeln, d.h. die Sperrlisten MÜSSEN von der jeweiligen CA ausgestellt werden und mindestens alle von dieser CA ausgestellten, gesperrten und noch gültigen Zertifikate enthalten. Darüber hinaus DÜRFEN sie auch von dieser CA ausgestellte, gesperrte und abgelaufene Zertifikate enthalten.

7.2.1 Versionsnummer(n)

Alle Sperrlisten MÜSSEN im Format X.509 Version 2 ausgestellt werden.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

Alle Sperrlisten MÜSSEN mindestens die Sperrlistenerweiterungen `AuthorityKeyIdentifier` und `cRLNumber` enthalten.

CARLs MÜSSEN die Sperrlisteneintragserweiterung `reasonCode` enthalten, CRLs DÜRFEN sie enthalten.

Wenn abgelaufene Zertifikate nicht aus der Sperrliste entfernt werden, MUSS die Sperrliste die Erweiterung `expiredCertsOnCRL` enthalten. Wenn abgelaufene Zertifikate aus der Sperrliste entfernt werden, DARF die Sperrliste die Erweiterung `expiredCertsOnCRL` NICHT enthalten.

[TLS] [SMIME] CRLs MÜSSEN die Sperrlisteneintragserweiterung `reasonCode` enthalten, wenn einer der folgenden Sperrgründe vorliegt (siehe dazu auch Kap. 4.9.1.2):

- `keyCompromise`
- `privilegeWithdrawn`
- `cessationOfOperation`
- `affiliationChanged`
- `superseded`

Wenn der Sperrgrund keinem der o.g. Sperrgründe entspricht, DARF die Sperrlisteneintragserweiterung `reasonCode` NICHT gesetzt werden.

Alle Erweiterungen DÜRFEN NICHT als kritisch markiert werden.

7.3 OCSP-Profil

Alle OCSP-Antworten MÜSSEN den Anforderungen des [RFC6960] genügen und entweder von der CA selbst oder einem OCSP-Signer signiert werden, dessen Zertifikat von der CA ausgestellt wurde.

Wenn die OCSP-Antworten durch einen eigens dafür vorgesehenen OCSP-Signer signiert werden, so MUSS gemäß [RFC6960] für das OCSP-Signer-Zertifikat eine der folgenden Varianten gewählt werden:

- Es wird dem OCSP-Signer für die Lebensdauer des OCSP-Signer-Zertifikats vertraut. In diesem Fall MUSS die Erweiterung `id-pkix-ocsp-nocheck` im OCSP-Signer-Zertifikat gesetzt werden und den Wert `NULL` enthalten. Die Erweiterungen `cRLDistribution-Points` und `authorityInfoAccess` SOLLTEN in diesem Fall NICHT gesetzt werden und das OCSP-Signer-Zertifikat SOLLTE aufgrund der fehlenden Prüfmöglichkeit seines Status eine kurze Gültigkeitsdauer haben und regelmäßig erneuert werden.
- Es wird eine Prüfmöglichkeit des OCSP-Signer-Zertifikats in den Erweiterungen `cRLDistributionPoints` und/oder `authorityInfoAccess` festgelegt.
- Es wird keine Methode zu Prüfung des Status des OCSP-Signers definiert und somit dem Prüfenden die Entscheidung überlassen, ob und wie er den Status des OCSP-Signer-Zertifikats prüft.

Für die Signatur der OCSP-Antworten MÜSSEN die in Kap. 7.1.3 aufgeführten Algorithmen verwendet werden.

[TLS] [SMIME] Wenn die OCSP-Antworten durch einen eigens dafür vorgesehenen OCSP-Signer signiert werden, so MUSS für das OCSP-Signer-Zertifikat die erste der oben aufgeführten Varianten gewählt werden.

[TLS] [SMIME] OCSP-Antworten zu gesperrten Sub-CA oder Cross-Zertifikaten MÜSSEN den Sperrgrund im `revocationReason` innerhalb der `revokedInfo` (nicht in den Erweiterungen, siehe Kap. 7.3.2) enthalten. Bzgl. der Sperrgründe gelten die in Kap. 7.2.2 getroffenen Festlegungen.

7.3.1 Versionsnummer(n)

Es MUSS OCSP in der Version 1 gemäß [RFC6960] eingesetzt werden.

7.3.2 OCSP-Erweiterungen

Keine Vorgabe.

[TLS] [SMIME] Die Erweiterung `reasonCode` gemäß [RFC5280#5.3.1] DARF in OCSP-Antworten NICHT gesetzt werden (siehe dazu auch Kap. 7.3).

[QCP] Die Erweiterung `archiveCutOff` SOLLTE in der Antwort mit dem Zeitpunkt des Gültigkeitsbeginns des referenzierten CA-Zertifikats gesetzt werden.

8 AUDITS UND ANDERE BEWERTUNGS-KRITERIEN

8.1 Häufigkeit und Art der Prüfungen

8.1.1 Selbstüberprüfung

Keine Vorgabe.

[TLS] [SMIME] Im gesamten Zeitraum, in dem Endteilnehmerzertifikate ausgestellt werden, MÜSSEN durch geeignete Selbstüberprüfungen die Einhaltung der Vorgaben dieser CP und der anwendbaren CPS sowie ihre Servicequalität kontrolliert werden. Diese Selbstüberprüfungen MÜSSEN mindestens vierteljährlich erfolgen und MÜSSEN stichprobenartig eine zufällige Auswahl von mindestens drei Prozent der Endteilnehmerzertifikate umfassen, die seit der letzten Selbstüberprüfung ausgestellt wurden.

[SMIME] Sofern weniger als 1.000 Zertifikate ausgestellt wurden, MÜSSEN mindestens 30 Zertifikate überprüft werden.

[EVCP] Es MÜSSEN mindestens 6% der Zertifikate überprüft werden.

Des Weiteren MÜSSEN mindestens vierteljährlich Zertifikate geprüft werden, welche von delegierten Dritten ausgestellt wurden oder Informationen enthalten, welche von delegierten Dritten geprüft wurden, es sei denn, der delegierte Dritte wird selbst gemäß Kap. 8.1.2 geprüft. Für diese Prüfung MUSS ein Validierungsspezialist des TSP eingesetzt werden.

Darüber hinaus MÜSSEN die Praktiken und Verfahren aller delegierten Dritten mindestens jährlich bzgl. der Einhaltung der Anforderungen dieser CP und der anwendbaren CPS überprüft werden.

8.1.2 Prüfungen durch externe Auditoren

Keine Vorgabe.

[TLS] [SMIME] Die Trust Services MÜSSEN in einer ununterbrochenen Folge von Audit-Perioden von der Erzeugung eines CA-Schlüsselpaares bis zu dessen Zerstörung und dem Entzug des Vertrauens ("Cradle-to-Grave") gemäß eines in Kap. 8.4 gelisteten Auditschemas geprüft werden („Period-of-time-Audits“), dabei DARF eine Periode die Zeitdauer von einem Jahr NICHT überschreiten.

[3145] Die Trust Services MÜSSEN jährlich gemäß Kap. 8.4 geprüft werden.

[QCP] Die Trust Services MÜSSEN mindestens alle 24 Monate von einer Konformitätsbewertungsstelle geprüft werden.

8.1.3 Prüfungen von Unterauftragnehmern und delegierten Dritten

Keine Vorgabe.

[TLS] Es MUSS überprüft werden, ob beauftragte Dritte die Anforderungen für die Aufbewahrung von Dokumenten und die Protokollierung von Ereignissen gemäß Kap. 5.4.1 erfüllen.

[3145] Unterauftragnehmer oder delegierte Dritte MÜSSEN in den anwendbaren Bereichen in demselben Umfang gemäß den Anforderungen aus [3145] geprüft werden, wie der Betrieb des TSP selbst. Diese Anforderung MUSS vertraglich mit den Unterauftragnehmern oder delegierten Dritten vereinbart werden.

8.2 Identität/Qualifikation der Prüfer

Interne Auditoren, welche die Selbstüberprüfungen gemäß Kap. 8.1.1 sowie die Prüfungen von Unterauftragnehmern und delegierten Dritten gemäß Kap. 8.1.3 durchführen, MÜSSEN über hinreichende Erfahrung als Auditoren und Expertise zu PKI-Technologien und -Prozessen verfügen.

Bei den externen Prüfern, welche die Prüfungen gemäß Kap. 8.1.2 durchführen, MUSS es sich um qualifizierte Auditoren handeln, die über folgende Qualifikationen und Fähigkeiten verfügen:

- Sie MÜSSEN unabhängig vom Prüfgegenstand sein.
- Sie MÜSSEN Prüfungen durchführen können, welche die in geeigneten Prüfungsschemata gemäß Kap. 8.4 festgelegten Kriterien erfüllen.
- Sie MÜSSEN Personen beschäftigen, die kompetent in der Prüfung von PKI-Technologien, Informationssicherheits-Tools und -Techniken, Informationstechnologien und Sicherheitsüberprüfungen sind und die Funktion der Bestätigung als Drittpartei beherrschen.
- Sie MÜSSEN durch Gesetz, staatliche Vorschriften oder berufsethische Regeln gebunden sein.

Für Prüfungen nach ETSI MUSS die Prüfstelle gemäß ISO 17065 unter Anwendung der in ETSI EN 319 403 festgelegten Anforderungen durch die „Deutsche Akkreditierungsstelle“ (DAkkS) akkreditiert und Mitglied des „Accredited Conformity Assessment Bodies‘ Council“ (ACAB’c) sein.

[TLS] [SMIME] Externe Prüfer MÜSSEN darüber hinaus eine Berufshaftpflicht-, Fehler- und Unterlassungsversicherung mit einer Deckungssumme von mindestens einer Million US-Dollar unterhalten.

[QCP] Die TSP MÜSSEN von Konformitätsbewertungsstellen geprüft werden, welche die Voraussetzungen aus ETSI EN 319 403 erfüllen.

[3145] Die Audits MÜSSEN von ISO 27001 Auditoren durchgeführt werden.

8.3 Beziehung des Prüfers zur geprüften Stelle

Externe Prüfer, welche die Prüfungen gemäß Kap. 8.1.2 durchführen, MÜSSEN unabhängig von der geprüften Stelle und dem Prüfgegenstand sein.

Für interne Auditoren MUSS die Rollentrennung gemäß Kap. 5.2.4 beachtet werden.

8.4 Abgedeckte Bereiche der Prüfung

Keine Vorgabe.

[TLS] [SMIME] Die Trust Services MÜSSEN nach ETSI EN 319 411-1 bzw. -2 in der jeweils aktuellen Version geprüft werden.

[TLS] Anwendbare Policies sind

- DVCP,
- OVCP oder
- QNCP-w.

[SMIME] Anwendbare Policies sind

- LCP,
- NCP oder
- NCP+.

[EVCP] Anwendbare Policies sind

- EVCP oder
- QEVCP-w

Die Prüfungen MÜSSEN alle CAs umfassen. In der Prüfdokumentation MÜSSEN alle geprüften PKI-Hierarchien dokumentiert werden.

[QCP] Die Trust Services MÜSSEN gemäß ETSI EN 319 411-2 in der jeweils aktuellen Version geprüft werden.

Anwendbare Policies sind:

- QCP-n,
- QCP-l,
- QCP-n-qscd,
- QCP-l-qscd,
- QEVCP-w oder
- QNCP-w.

Darüber hinaus MUSS eine Konformitätsbewertung gemäß [eIDAS] durchgeführt werden.

[3145] Der Auditprozess MUSS das ISMS und die Anforderungen der [TR3145] umfassen

8.5 Maßnahmen infolge von Mängeln

Mängel MÜSSEN in den von den Prüfern festgelegten Fristen beseitigt werden.

[TLS] [SMIME] Mängel, die gegen die [BR], [EVCG], [MSRP], [MOZRP], [GCRP] oder [APLRP] verstoßen, MÜSSEN den betroffenen Root-Store-Betreibern gemeldet werden. Sofern fehlerhafte Zertifikate bemängelt werden, MÜSSEN die Sperrgründe und -fristen gemäß Kap. 4.9.1 berücksichtigt werden.

8.6 Mitteilung der Ergebnisse

Keine Vorgabe.

[TLS] [SMIME] Die Links zu den von den externen Prüfern erstellten und veröffentlichten Audit-Bescheinigungen MÜSSEN in der „Common CA Database“ (CCADB) veröffentlicht werden.

Diese Bescheinigungen SOLLTEN innerhalb von drei Monaten nach Ende der Prüfung veröffentlicht werden. Im Falle einer Veröffentlichung nach mehr als drei Monaten MUSS ein von dem externen Prüfer unterzeichnetes Erläuterungsschreiben vorgelegt werden.

Die externen Prüfer MÜSSEN bei der Erstellung der Audit-Bescheinigungen die Vorgaben an die Form und Inhalte aus [CCADB#5.1] („Audit Statement Content“) berücksichtigen.

[QCP] Die TSP MÜSSEN die Konformitätsbewertungsberichte der Prüfungen gemäß Kap. 8.1.2 innerhalb von drei Tagen nach Erhalt der zuständigen Aufsichtsbehörde vorlegen.

9 SONSTIGE GESCHÄFTLICHE UND RECHTLICHE BESTIMMUNGEN

9.1 Entgelte

9.1.1 Gebühren für die Ausstellung oder Erneuerung von Zertifikaten

Keine Vorgabe.

9.1.2 Gebühren für den Zertifikatszugang

Keine Vorgabe.

9.1.3 Gebühren für den Zugang zu Sperr- oder Statusinformationen

Keine Vorgabe.

[QCP] Statusinformationen MÜSSEN kostenfrei bereitgestellt werden.

9.1.4 Gebühren für andere Dienstleistungen

Keine Vorgabe.

9.1.5 Rückerstattungsrichtlinie

Keine Vorgabe.

9.2 Finanzielle Verantwortlichkeiten

Die TSP MÜSSEN über die finanzielle Stabilität und Ressourcen verfügen, die zu einem zu dieser CP konformen Betrieb inkl. einer geplanten Einstellung gemäß Kap. 5.8 erforderlich sind. Darüber hinaus MÜSSEN die TSP, soweit dies im Rahmen der geltenden Insolvenzgesetze möglich ist, Vereinbarungen zur Deckung der Kosten treffen, um die Mindestanforderungen gemäß Kap. 5.8 im Insolvenzfall erfüllen zu können.

9.2.1 Versicherungsschutz

Die TSP MÜSSEN über eine angemessene Haftpflichtversicherung gemäß geltendem Recht verfügen, wenn sie nicht über hinreichende finanzielle Ressourcen zur Absicherung etwaiger Haftungsforderungen aufgrund vorsätzlicher oder fahrlässiger Handlungen verfügen.

[EVCP] Die TSP MÜSSEN in Bezug auf ihre Leistungen und Verpflichtungen gemäß dieser CP über folgende Haftpflichtversicherung(en) verfügen:

- Eine allgemeine Haftpflichtversicherung mit einer Deckungssumme von mindestens 2 Mio. US-Dollar, sowie
- eine Berufshaftpflichtversicherung mit einer Deckungssumme von mindestens 5 Mio. US-Dollar, welche Schadensersatzansprüche aufgrund
  - einer Handlung, eines Fehlers oder einer Unterlassung,
  - einer unbeabsichtigten Vertragsverletzung,
  - einer Vernachlässigung bei der Ausstellung oder dem Betrieb von EV-Zertifikaten,
  - einer Verletzung der Eigentumsrechte Dritter (ausgenommen Urheberrechts- und Markenrechtsverletzung),
  - einer Verletzung der Privatsphäre oder
  - einer Verletzung der Werbung

  abdeckt.

Diese Versicherung MUSS bei einem Unternehmen abgeschlossen sein, das in der aktuellen Ausgabe des „Best's Insurance Guide“ ein Rating von mindestens „A“ aufweist.

9.2.2 Sonstige Vermögensgegenstände

Keine Vorgabe.

9.2.3 Versicherungs- oder Garantiedeckung für Endteilnehmer

Keine Vorgabe.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Umfang an vertraulichen Informationen

Keine Vorgabe.

9.3.2 Umfang an nicht vertraulichen Informationen

Keine Vorgabe.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Vertrauliche Geschäftsinformationen MÜSSEN ihrer Klassifizierung entsprechend angemessen geschützt werden.

9.4 Schutz von personenbezogenen Daten

9.4.1 Datenschutzkonzept

Zum Schutz personenbezogener Daten MUSS die [DSGVO] beachtet werden.

Es MÜSSEN geeignete technische und organisatorische Maßnahmen

- zur Wahrung der Integrität und Vertraulichkeit bei der Übermittlung und Speicherung,
- gegen eine unerlaubte oder unrechtmäßige Verarbeitung,
- gegen einen zufälligen Verlust oder die zufällige Zerstörung oder Beschädigung

dieser Daten ergriffen werden.

In den Datenschutzkonzepten MUSS beschrieben werden, wie die Vorgaben der [DSGVO] bzgl. der im Registrierungsprozess erhobenen Daten umgesetzt werden.

Daten, die zur Erbringung der Dienstleistung nicht relevant oder angemessen sind, DÜRFEN NICHT erhoben werden.

Die relevanten Informationen bzgl. der Verarbeitung, Speicherung, Löschung und ggf. Archivierung der erfassten Daten, sowie Kontaktinformationen zur Ausübung der Datenschutzrechte MÜSSEN in Datenschutzerklärungen veröffentlicht werden.

In den CPS MUSS in Kap. 9.4.1 beschrieben werden, wo die Datenschutzerklärungen eingesehen werden können.

9.4.2 Als privat zu behandelnde Informationen

Alle personenbezogenen Daten, die nicht in Zertifikaten veröffentlicht werden sollen oder bereits anderweitig veröffentlicht worden sind, MÜSSEN als privat behandelt werden. Dazu gehört auch die Information über die wahre Identität eines Pseudonyms.

9.4.3 Nicht als privat geltende Informationen

Keine Vorgabe.

9.4.4 Verantwortung für den Schutz privater Informationen

Keine Vorgabe.

9.4.5 Benachrichtigung und Zustimmung zur Verwendung privater Informationen

Keine Vorgabe.

9.4.6 Offenlegung im Rahmen eines Gerichts- oder Verwaltungsverfahrens

Keine Vorgabe.

9.4.7 Andere Umstände der Offenlegung von Informationen

Keine Vorgabe.

9.5 Urheberrecht

Keine Vorgabe.

9.6 Zusicherungen und Gewährleistungen

9.6.1 Zusicherungen und Gewährleistungen der TSP

Die TSP MÜSSEN zuverlässig sein und ihre Trust Services auf vertrauenswürdige und legale Art und Weise konform zu dieser CP und ihren CPS betreiben.

Die TSP MÜSSEN die Gesamtverantwortung für die Einhaltung der Konformität zu dieser CP und ihren CPS auch dann behalten, wenn sie Tätigkeiten an Unterauftragnehmer oder Dritte, z.B. Anbieter von Vertrauensdienstkomponenten oder externen RAs, auslagern. Dazu MÜSSEN die Aufgaben der Dritten und die damit verbundenen Verfahrensweisen, Verantwortlichkeiten und Haftungsbedingungen festgelegt werden und die Dritten MÜSSEN vertraglich verpflichtet werden, alle geforderten Maßnahmen umsetzen. Die Verpflichtungen der Dritten MÜSSEN in den CPS beschrieben werden.

Wenn von einem Anbieter bereitgestellte Vertrauensdienstkomponenten verwendet werden, MUSS sichergestellt werden,

- dass die Verwendung der Schnittstelle der Komponente den vom Anbieter der Vertrauensdienstkomponente festgelegten Anforderungen entspricht,
- dass die von der Vertrauensdienstkomponente geforderte Sicherheit und Funktionalität den entsprechenden Anforderungen dieser CP und dem relevanten CPS entsprechen.

Wenn Datenbestände unabhängiger Dritter zur Validierung von Daten verwendet werden („QIIS“, siehe Kap. 3.2.2), MÜSSEN diese im Hinblick auf ihre Zuverlässigkeit, Genauigkeit sowie ihre Änderungs- oder Fälschungssicherheit evaluiert werden. Dabei MUSS Folgendes berücksichtigt werden:

- Alter der vorgelegten Informationen
- Häufigkeit der Aktualisierungen der Informationsquelle
- Datenanbieter und der Zweck der Datenerfassung
- Verfügbarkeit der Daten
- Integrität der Daten (d.h. die relative Schwierigkeit, diese zu fälschen oder zu verändern)

Von den TSP oder deren Beteiligungsgesellschaften selbst gepflegte Datenbanken DÜRFEN NICHT als zuverlässige Datenquellen angesehen werden, wenn der Hauptzweck der Datenbanken darin liegt, Informationen zur Erfüllung der Validierungsanforderungen zu sammeln.

Die Trust Services DÜRFEN NICHT diskriminierend sein und SOLLTEN allen Antragstellern zugänglich gemacht werden,

- deren Tätigkeiten in den von den Diensten angegebenen Tätigkeitsbereich fallen und
- die sich damit einverstanden erklären, ihren in den Geschäftsbedingungen des TSP festgelegten Verpflichtungen nachzukommen.

Die den Zertifikatsnehmern angebotenen Dienste und Produkte MÜSSEN soweit möglich auch Menschen mit Behinderungen zugänglich gemacht werden, anwendbare Standards zur Barrierefreiheit aus ETSI EN 301 549 SOLLTEN berücksichtigt werden.

Dritten MUSS die Möglichkeit geboten werden, alle angebotenen Zertifikatstypen zu überprüfen und zu testen.

[TLS] [SMIME] Telekom Security als Betreiber der Root CAs ist verantwortlich für

- die Leistungen und Gewährleistungen der TSP,
- die Einhaltung dieser CP durch die TSP,
- alle Verbindlichkeiten und Freistellungsverpflichtungen der TSP gemäß [BR].

Für jedes ausgestellte Zertifikat MUSS sowohl den Endteilnehmern, den relevanten Root Store Betreibern, als auch allen vertrauenden Dritten garantiert werden, dass

- der Zertifikatsnehmer das Recht hat, die im `subjectDN` und/oder `subjectAltName` aufgeführten Domain-Namen, IP-Adressen oder E-Mail-Adressen zu verwenden,
- sofern anwendbar, der Vertreter des Zertifikatsnehmers autorisiert war, das Zertifikat im Namen des Zertifikatsnehmers zu beantragen,
- sie von den Zertifikatsnehmern zur Ausstellung der Zertifikate autorisiert waren,
- die Richtigkeit aller im Zertifikat aufgenommenen Inhalte,
- der Antragsteller gemäß Kap. 3.2 identifiziert wurde,
- sie, sofern der Zertifikatsnehmer nicht mit dem TSP verbunden ist, mit dem Zertifikatsnehmer einen rechtsgültigen und durchsetzbaren Vertrag, der alle relevanten Anforderungen erfüllt, abgeschlossen haben,
- sofern der Zertifikatsnehmer mit dem TSP verbunden ist, ein Vertreter des Zertifikatsnehmers die Nutzungsbedingungen anerkannt hat,
- sie mindestens bis zum Ablaufdatum des Zertifikats Statusdienste gemäß Kap. 4.10 betreiben und Statusinformationen rund um die Uhr öffentlich bereitstellen,
- sie ein Zertifikat bei Vorliegen eines der im CPS aufgeführten Sperrgründe sperren,
- sie während der gesamten Gültigkeitsdauer eines Zertifikats die Anforderungen dieser CP sowie ihrer eigenen CPS einhalten.

Die zur Einhaltung der vorgenannten Zertifikatsgarantien erforderlichen Prozesse und Maßnahmen MÜSSEN in den CPS beschrieben werden.

Die Verträge mit den Zertifikatsnehmern inkl. der Nutzungsbedingungen (siehe Kap. 9.6.3) MÜSSEN rechtlich durchsetzbar sein.

[EVCP] Für jedes ausgestellte EV-Zertifikat MUSS gewährleistet werden, dass

- über eine Gründungs- oder Registrierungsagentur in der Gründungs- oder Registrierungsgerichtsbarkeit des Zertifikatsnehmers geprüft wurde, dass der Zertifikatsnehmer als rechtlich gültige Organisation oder gültiges Unternehmen existiert,
- der Name des Zertifikatsnehmers zum Zeitpunkt der Ausstellung des Zertifikats mit dem Namen in den offiziellen Registrierungsunterlagen übereinstimmt,
- alle zumutbaren Schritte unternommen wurden, um zu überprüfen, ob
  - der Zertifikatsnehmer zum Zeitpunkt der Ausstellung des Zertifikats das Recht hat, alle im Zertifikat aufgeführten Domain Names zu verwenden,
  - der Antragsgenehmiger die Ausstellung des Zertifikats genehmigt hat,
  - alle anderen Informationen zum Zeitpunkt der Ausstellung des Zertifikats korrekt waren,
- mit dem Zertifikatsnehmer, sofern dieser nicht mit dem TSP verbunden ist, eine rechtsgültige und durchsetzbare Vereinbarung getroffen wurde, die alle Anforderungen aus [EVCG] berücksichtigt.

[QCP] Wenn private Schlüssel der Zertifikatsnehmer während der Gültigkeitsdauer der korrespondierenden Zertifikate vom TSP verwaltet werden, SOLLTE dies in den CPS beschrieben werden. Darüber hinaus DARF diese Information auch im Endteilnehmer-Zertifikat aufgeführt werden.

[3145] Wenn Dritte im Rahmen des Identifizierungs- und Registrierungsverfahrens Dienstleistungen für einen TSP erbringen, MÜSSEN diese das Sicherheitsniveau "hoch" und die Zuverlässigkeit sowie die Vertrauenswürdigkeit des eingesetzten Personals gewährleisten. Hierzu MUSS mit dem Dritten eine unterzeichnete Vereinbarung abgeschlossen werden, die darüber hinaus auch die im vorherigen Absatz aufgeführten Aspekte beinhaltet.

9.6.2 Zusicherungen und Gewährleistungen der RAs

Die Zusicherungen und Gewährleistungen der RAs MÜSSEN festgelegt und in den CPS beschrieben werden, dabei sind mindestens zu berücksichtigen:

- Antragsbearbeitung gemäß Kap. 4
- Organisatorische Maßnahmen gemäß Kap. 5.2
- Personelle Maßnahmen gemäß Kap. 5.3
- Archivierung von Unterlagen gemäß Kap. 5.5
- Technische Maßnahmen gemäß Kap. 6.5
- Datenschutzanforderungen gemäß Kap. 9.4

9.6.3 Zusicherungen und Gewährleistungen der Zertifikatsnehmer

Die Nutzungsbedingungen für die Endteilnehmer-Zertifikate MÜSSEN festgelegt werden und es MUSS von den Zertifikatsnehmern vor der Ausstellung der Zertifikate deren Akzeptanz bestätigt werden.

Diese Nutzungsbedingungen MÜSSEN mindestens folgende Verpflichtungen des Zertifikatsnehmers berücksichtigen:

a) eine Verpflichtung, dem TSP genaue und vollständige Informationen zu liefern,
b) eine Verpflichtung, alle angemessenen Maßnahmen zu ergreifen, um die Vertraulichkeit und Kontrolle über die privaten Schlüssel und Aktivierungsdaten zu gewährleisten,
c) eine Verpflichtung, das Schlüsselpaar nur in Übereinstimmung mit etwaigen Einschränkungen, die dem Zertifikatsnehmer mitgeteilt wurden, zu verwenden,
d) ein Verbot der unerlaubten Nutzung der privaten Endteilnehmer-Schlüssel,
e) eine Verpflichtung, ein Zertifikat unverzüglich zu sperren oder sperren zu lassen, wenn ein Sperrgrund gemäß Kap. 4.9.1.2 vorliegt.
f) eine Verpflichtung, nach Sperrung des Endteilnehmer-Zertifikats die Verwendung des korrespondierenden privaten Schlüssels, mit Ausnahme der Schlüsselentschlüsselung (sofern anwendbar), sofort und dauerhaft einzustellen,
g) eine Verpflichtung, nach Bekanntwerden der Kompromittierung der ausstellenden Sub-CA die Verwendung des privaten Endteilnehmer-Schlüssels, mit Ausnahme der Schlüsselentschlüsselung (sofern anwendbar), sofort und dauerhaft einzustellen,
h) für den Fall, dass ein Zertifikatsnehmer seine Schlüssel selbst generiert:
eine Verpflichtung zur Generierung der Schlüssel unter Verwendung geeigneter Algorithmen und Schlüssellängen gemäß Kap. 6.1.5,

i) für den Fall, dass ein Zertifikatsnehmer eine natürliche Person ist und seine Schlüssel selbst generiert und diese für eine „Verpflichtung zu signierten Inhalten“ (siehe Kap. 7.1.2 (05) bzgl. `keyUsage nonRepudiation`) genutzt werden:
eine Verpflichtung, dass der private Schlüssel unter der alleinigen Kontrolle des Zertifikatsnehmers aufbewahrt wird,

j) für den Fall, dass ein Zertifikatsnehmer eine Organisation ist und seine Schlüssel selbst generiert und diese für eine „Verpflichtung zu signierten Inhalten“ (siehe Kap. 7.1.2 (05) bzgl. `keyUsage nonRepudiation`) genutzt werden:
eine Verpflichtung, den privaten Schlüssel unter der Kontrolle des Organisation zu halten,

k) [NCP+] eine Verpflichtung, den privaten Schlüssel für kryptografische Funktionen nur innerhalb sicherer kryptografischer Module zu verwenden,

l) [NCP+] für den Fall, dass die Schlüssel unter der Kontrolle des Zertifikatsnehmers generiert werden: eine Verpflichtung, die Schlüssel innerhalb des sicheren kryptografischen Moduls zu generieren,

m) [TLS] eine Verpflichtung, das Zertifikat nur auf Servern zu installieren, auf die unter den im `subjectAltName` aufgeführten Namen zugegriffen werden kann,

n) [SMIME] eine Verpflichtung, das Zertifikat nur für die im Zertifikat aufgeführten Mailbox-Adressen zu verwenden,

o) [TLS] [SMIME] eine Verpflichtung, den Inhalt des Zertifikats auf Richtigkeit zu überprüfen,

p) [TLS] [SMIME] eine Verpflichtung, das Zertifikat ausschließlich in Übereinstimmung mit allen geltenden Gesetzen und in Übereinstimmung mit der abgeschlossenen Vereinbarung und den Nutzungsbedingungen zu nutzen,

q) [TLS] [SMIME] eine Verpflichtung, innerhalb eines bestimmten Zeitraums auf die Anweisungen des TSP bei Kompromittierung eines Schlüssels oder Zertifikatsmissbrauch zu reagieren,

r) [TLS] [SMIME] eine Verpflichtung zu akzeptieren, dass ein TSP berechtigt ist, ein Zertifikat sofort zu sperren, wenn ein Sperrgrund gemäß Kap. 4.9.1.2 vorliegt,

s) [3145] eine Verpflichtung, jede Änderung der Registrierungsdaten dem TSP mitzuteilen und spätestens nach Ablauf der unter rr) festgelegten Frist zu bestätigen, dass die Registrierungsdaten noch gültig sind,

t) [3145] für den Fall, dass ein Zertifikatsnehmer die Schlüssel selbst generiert: eine Verpflichtung, die Schlüssel gemäß den Vorgaben (siehe Kap. 6.1.5 und 6.1.6) zu generieren und aufzubewahren),

u) [3145] für den Fall, dass die TSP die Schlüssel der Zertifikatsnehmer auf Token generieren und übergeben: eine Verpflichtung zur Meldung einer Kompromittierung der Aktivierungsdaten im Rahmen der Tokenübergabe, was zu einer Sperrung des Zertifikats führt,

v) [3145] eine Verpflichtung, das Endteilnehmer-Zertifikat sowie das ausstellende Sub-CA-Zertifikat zu prüfen,

x) [QCP-n-qscd] eine Verpflichtung, den Schlüssel unter seiner alleinigen Kontrolle zu halten,

y) [QCP-l-qscd] eine Verpflichtung, den Schlüssel unter der Kontrolle der Organisation zu halten,

z) [QCP-n-qscd] eine Verpflichtung, den Schlüssel ausschließlich zur Erzeugung elektronischer Signaturen zu nutzen,

aa) [QCP-l-qscd] eine Verpflichtung, den Schlüssel ausschließlich zur Erzeugung elektronischer Siegel zu nutzen.

Darüber hinaus MÜSSEN die Nutzungsbedingungen Informationen zu folgenden Aspekten enthalten:

bb) sofern anwendbar, die anwendbare Policy gemäß ETSI EN 319 411-1 bzw. -2
cc) eine Information, was als Akzeptanz des Zertifikats gilt
dd) der Zeitraum, über den die Aufzeichnungen (siehe Kap. 5.5.2) aufbewahrt werden
ee) Anforderungen an vertrauende Dritte gemäß Kap. 9.6.4
ff) ob und wenn ja, auf welche Art und Weise die Anforderungen dieser CP ergänzt oder weiter eingeschränkt werden
gg) alle Beschränkungen der Nutzung des angebotenen Dienstes
hh) Haftungsbeschränkungen der TSP
ii) anwendbares Recht
jj) Verfahren bei Beschwerden und zur Streitbeilegung
kk) Häufigkeit und zugrundeliegende Auditschemata der Auditierungen der TSP gemäß Kap. 8.1 und 8.4
ll) Kontaktinformationen des TSP
mm) Aussagen zur Verfügbarkeit der bereitgestellten Dienste
nn) auszuwählende Sperrgründe bei Sperrung durch den Zertifikatsnehmer
oo) [3145] die Art und Weise, wie die Zertifikatsnehmer die Registrierungsdaten übertragen können,
pp) [3145] Regelungen zur Akzeptanz neuer Versionen der Nutzungsbedingungen durch die Zertifikatsnehmer außerhalb der Antragsprozesse in Übereinstimmung mit den geltenden Gesetzen,
qq) [3145] eine Definition der verschiedenen Rollen der Zertifikatsnehmer, der verschiedenen möglichen Subjekte eines Zertifikats, sowie weiterer bedeutender Rollen in den Zertifikatsmanagementprozessen (siehe Kap. 1.3.3),
rr) [3145] eine Frist, nach deren Ablauf die Zertifikatsnehmer bestätigen müssen, dass ihre Registrierungsdaten weiterhin gültig sind,
ss) [3145] weitere Vorgaben an die Zertifikatsnehmer in Abhängigkeit des geforderten Sicherheitsniveaus (z.B. Virenschutz, Firewalls Sicherheitsupdates der Betriebssysteme, angemessener Schutz der Schlüssel und Aktivierungsdaten, Nutzung von sicheren kryptografischen Modulen bei hohem Sicherheitsniveau),
tt) [3145] für den Fall, dass ein Zertifikatsnehmer die Schlüssel selbst generiert: die Anforderungen an die zur Schlüsselgenerierung verwendete Hard- und Software,
uu) [3145] für den Fall, dass die TSP die Schlüssel der Zertifikatsnehmer generieren: der Prozess der Schlüsselübergabe,
vv) [3145] für den Fall, dass die TSP die Schlüssel der Zertifikatsnehmer auf Token generieren und übergeben: der Prozess der Übergabe der Token,
ww) [3145] die Voraussetzungen für eine Zertifikatserneuerung mit oder ohne Schlüsselwechsel sowie für die Ausstellung eines Ersatzzertifikats,
xx) [3145] Die Zeiträume und Umstände, unter denen eine Änderung von Zertifikatsdaten erlaubt oder erforderlich ist,
yy) [3145] Informationen über den Prozess der Beendigung eines TSP oder einer RA (siehe Kap. 5.8),
zz) [3145] Informationen über die Fristen der regelmäßigen Updates der Statusdienste.
aaa) [VS-NfD] Einstufung des Schlüsselmaterials nach [SÜG] und [VSA]

Für den Fall, dass der Zertifikatsnehmer nicht zugleich das Subjekt des Zertifikats ist und das Subjekt des Zertifikats kein Gerät ist, MÜSSEN

1) für das Subjekt des Zertifikats die o.g. Verpflichtungen c), d), e), f), g), i) j) und k) gelten und für den Fall, dass das Subjekt des Zertifikats eine Person ist, diese darüber informiert werden,
2) die Vereinbarung mit dem Zertifikatsnehmer aus zwei Teilen bestehen:
   a) Der erste Teil MUSS vom Zertifikatsnehmer unterzeichnet bzw. bestätigt werden und MUSS folgende Aspekte berücksichtigen:
      i) Zustimmung zu den Verpflichtungen des Zertifikatsnehmers
      ii) Zustimmung zur Nutzung eines sicheren kryptografischen Moduls, sofern gefordert
      iii) Zustimmung zur Verarbeitung der erhobenen Daten und, sofern anwendbar, die Weitergabe dieser Daten an vom TSP beauftragte Dritte, inkl. einer Weitergabe der Daten im Falle einer Beendigung des Dienstes
      iv) Bedingungen zur Veröffentlichung des Zertifikats auf Verlangen des Zertifikatsnehmers unter Zustimmung des Subjekts des Zertifikats
      v) Bestätigung der Korrektheit aller im Zertifikat aufzunehmenden Daten
      vi) Verpflichtungen, die für das Subjekt des Zertifikats gelten (informativ)
   b) Der zweite Teil MUSS vom Subjekt des Zertifikats unterzeichnet bzw. bestätigt werden und MUSS folgende Aspekte berücksichtigen:
      i) Zustimmung zu den Verpflichtungen des Subjekts des Zertifikats (siehe 1))
      ii) Zustimmung zur Nutzung eines sicheren kryptografischen Moduls, sofern gefordert
      iii) Zustimmung zur Verarbeitung der erhobenen Daten und, sofern anwendbar, die Weitergabe dieser Daten an vom TSP beauftragte Dritte, inkl. einer Weitergabe der Daten im Falle einer Beendigung des Dienstes

Die Nutzungsbedingungen DÜRFEN in Form eines PDS gemäß Anhang A der [ETS411-1] bereitgestellt werden.

9.6.4 Zusicherungen und Gewährleistungen der Zertifikatsnutzer

In den Nutzungsbedingungen (siehe dazu auch Kap. 9.6.3) und/oder den PDS MÜSSEN folgende Empfehlungen für Zertifikatsnutzer aufgenommen werden:

Zertifikatsnutzer sollten

- die Gültigkeit der Zertifikate über die angebotenen Statusdienste gemäß Kap. 4.9.10 und 4.10 prüfen,
- die in den Nutzungsbedingungen oder im Zertifikat aufgeführten Beschränkungen zur Nutzung der Zertifikate berücksichtigen,
- alle weiteren Vorsichtsmaßnahmen treffen, die sich für Dritte aus Vereinbarungen oder anderweitigen Vorschriften ergeben.

9.6.5 Zusicherungen und Gewährleistungen sonstiger Teilnehmer

Keine Vorgabe.

9.7 Gewährleistungsausschlüsse

Keine Vorgabe.

9.8 Haftungsbeschränkungen

Die Haftung der TSP DARF im Einklang mit geltendem Recht beschränkt werden. Die Haftungsbeschränkungen MÜSSEN in den CPS sowie den Nutzungsbedingungen beschrieben werden, siehe dazu auch Kap. 9.6.3 Abs. hh).

[EVCP] Die Haftung der TSP DARF gegenüber Zertifikatsnehmern oder vertrauenden Dritten für rechtlich anerkannte und nachweisbare Ansprüche NICHT auf einen Geldbetrag von weniger als zweitausend US-Dollar pro Zertifikatsnehmer oder vertrauenden Dritten pro Endteilnehmer-Zertifikat beschränkt werden.

[QCP] Die TSP MÜSSEN gemäß Artikel 13 der EU-Verordnung 910/2014 („eIDAS“) für alle einer natürlichen Person oder Organisation vorsätzlich oder fahrlässig zugefügten Schäden haften.

9.9 Schadensersatz

Keine Vorgabe.

9.10 Laufzeit und Aufhebung dieser CP oder eines CPS

9.10.1 Laufzeit

Diese CP und alle darauf basierenden CPS haben eine Laufzeit von maximal einem Jahr, siehe dazu auch Kap. 9.12.

9.10.2 Aufhebung

Keine Vorgabe.

9.10.3 Auswirkungen der Beendigung und Fortführung

Keine Vorgabe.

9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Keine Vorgabe.

9.12 Änderungen an dieser CP oder einem CPS

9.12.1 Verfahren für Änderungen

Diese CP MUSS bei Bedarf, z.B. aufgrund geänderter Anforderungen oder relevanter Änderungen im Betrieb, spätestens aber innerhalb eines Jahres nach Inkrafttreten einem Review durch das PKI Compliance Management unterzogen werden.

Das PKI Compliance Management MUSS daher regelmäßig in angemessenen Abständen die zugrunde liegenden Anforderungen der in Anhang B referenzierten Dokumente auf neue Versionen überprüfen und die Aktivitäten in relevanten Foren verfolgen.

Änderungen an dieser CP sowie das jährliche Review MÜSSEN in der Änderungshistorie dieses Dokuments aufgeführt werden. Dies gilt auch für den Fall, dass beim jährlichen Review keine inhaltlichen Änderungen vorgenommen werden.

Neue Versionen dieser CP MÜSSEN gemäß Kap. 1.5.4 genehmigt werden und eine neue aufsteigende Versionsnummer erhalten.

Analog MÜSSEN die CPS aufgrund geänderter Anforderungen oder relevanter Änderungen im Betrieb, mindestens aber einmal pro Jahr einem Review durch die Trust Services unterzogen werden. Bzgl. der Änderungshistorie, Genehmigungsverfahren und Versionierung gilt das oben gesagte.

Bei Änderungen an den CPS, die sich auf die Nutzungsbedingungen auswirken, MÜSSEN die Nutzungsbedingungen angepasst und in einer neuen Version bereitgestellt werden.

9.12.2 Benachrichtigungsmechanismus und -zeitraum

Neue Versionen dieser CP MÜSSEN gemäß Kap. 2.2 veröffentlicht werden. Spätestens mit der Veröffentlichung einer neuen Version MÜSSEN alle betroffenen Trust Services informiert werden.

Neue Versionen eines CPS oder der Nutzungsbedingungen MÜSSEN gemäß Kap. 2.2 veröffentlicht werden. Spätestens mit der Veröffentlichung einer neuen Version MÜSSEN alle betroffenen Mitarbeiter des Trust Services informiert werden.

Zertifikatsnehmer und, sofern anwendbar die Zertifikatsnutzer, MÜSSEN über neue Versionen der Nutzungsbedingungen informiert werden, sofern diese neue oder geänderte Bedingungen enthalten, welche sich auch auf die Nutzung bereits ausgestellter Zertifikate bzw. Schlüssel auswirken. Bei Bekanntgabe der Änderungen DARF bzgl. der Details auf geänderte Dokumente im Repository verwiesen werden.

[3145] Vom Zertifikatsnehmer MUSS die Akzeptanz neuer Nutzungsbedingungen, welche neue oder geänderte Bedingungen enthalten, die sich auch auf die Nutzung bereits ausgestellter Zertifikate bzw. Schlüssel auswirken, eingeholt werden. Bzgl. der Regelungen zur Akzeptanz neuer Nutzungsbedingungen außerhalb der Antragungsprozesse siehe Kap. 9.6.3 pp).

[QCP] Neue Versionen einer CPS MÜSSEN den Aufsichtsbehörden übermittelt werden.

9.12.3 Umstände, unter denen die OID geändert werden muss

Wenn sich an dieser CP oder an einer CPS Änderungen ergeben, welche sich auf die Anwendbarkeit des jeweiligen Dokuments auswirken, SOLLTE das Dokument eine neue OID bekommen.

9.13 Bestimmungen zur Beilegung von Streitigkeiten

Richtlinien und Verfahren zur Beilegung von Beschwerden und Streitigkeiten, die von den Endteilnehmern oder vertrauenden Dritten zu den bereitgestellten Diensten eingehen, MÜSSEN festgelegt und in den CPS sowie den Allgemeinen Geschäftsbedingungen oder den Nutzungsbedingungen beschrieben werden.

9.14 Geltendes Recht

In den CPS MUSS das deutsche Recht als geltendes Recht festgelegt werden.

9.15 Einhaltung geltenden Rechts

Die TSP MÜSSEN sicherstellen, dass sie geltendes Recht einhalten und bei Bedarf Nachweise darüber vorlegen, wie sie die geltenden rechtlichen Anforderungen erfüllt.

9.16 Verschiedene Bestimmungen

9.16.1 Gesamte Vereinbarung

Keine Vorgabe.

9.16.2 Zuordnung

Keine Vorgabe.

9.16.3 Salvatorische Klausel

Keine Vorgabe.

[TLS] Im Falle eines Konflikts zwischen [BR] oder [SBR] und einem Gesetz DARF eine widersprüchliche Anforderung so weit modifiziert werden, wie es notwendig ist, um die Anforderung gültig und legal zu machen. Dies gilt nur für Operationen oder Zertifikatsausstellungen, die diesem Gesetz unterliegen. In einem solchen Fall MUSS in Kap. 9.16.3 des betroffenen CPS ein detaillierter Verweis auf das Gesetz, das eine Änderung dieser Anforderungen gemäß diesem Abschnitt erfordert, sowie die durchgeführte spezifische Änderung dieser Anforderungen aufgenommen werden. Vor der Ausstellung eines Zertifikats gemäß der geänderten Anforderung MUSS das CA/Browser Forum über die relevanten Passagen des geänderten Kapitels informiert werden (siehe dazu [BR#9.16.3] bzw. [SBR#9.16.3]).

Die vorgenommenen Modifikationen MÜSSEN eingestellt werden, sobald das für diese Modifikation herangezogene Gesetz nicht mehr gilt oder die Anforderungen der [BR] oder [SBR] so geändert wurden, dass es möglich ist, sie und das Gesetz gleichzeitig zu erfüllen. Eine angemessene Änderung der Praxis, eine Änderung des CPS des TSP und eine Mitteilung an das CA/Browser Forum MÜSSEN innerhalb von 90 Tagen erfolgen.

9.16.4 Rechtsdurchsetzung

Keine Vorgabe.

9.16.5 Höhere Gewalt

Keine Vorgabe.

9.17 Sonstige Bestimmungen

Keine Vorgabe.

ANHANG

Anhang A: Abkürzungen

Hinweis: Aufgrund der internationalen Standardisierung verbergen sich hinter den Abkürzungen meist englische Fachbegriffe, auf deren Übersetzung in die deutsche Sprache an dieser Stelle verzichtet wird.

Tabelle 4 - Abkürzungen

Abkürzung	Bedeutung
AATL	Adobe Approved Trust List
ADN	Authorization Domain Name
ARL	Authority Revocation List (siehe CARL)
ASN.1	Abstract Syntax Notation One
BR	Baseline Requirements
CA	Certification Authority
CAA	Certification Authority Authorization
CAB Forum	CA/Browser Forum
CARL	Certification Authority Revocation List
CCADB	Common CA Database
ccTLD	Country Code Top-Level Domain
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DAkkS	Deutsche Akkreditierungsstelle (German Accreditation Body)
DNS	Domain Name System
DVCP	Domain Validation Certificate Policy
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
eIDAS	electronic IDentification, Authentication and Trust Services
EKU	Extended Key Usage
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Extended Validation
EVCG	Extended Validation Certificate Guidelines
EVCP	Extended Validation Certificate Policy
FIPS	Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
gTLD	Generic Top-Level Domain
HSM	Hardware Security Module
ICANN	Internet Corporation for Assigned Names and Numbers
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission

IETF	Internet Engineering Task Force
IPS	Intrusion-Prevention-System
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITU	International Telecommunications Union
IVCP	Individual Validation Certificate Policy
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
MGF	Mask Generation Function
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVCP	Organizational Validation Certificate Policy
PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PSS	Probabilistic Signature Scheme
QCP	Qualified Certificate Policy
QCP-l	Policy for EU qualified certificate issued to a legal person
QCP-l-qscd	Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD
QCP-n	Policy for EU qualified certificate issued to a natural person
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD
QCP-w	Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person (veraltet)
QEVCP-w	Policy for EU qualified website certificate issued to a legal person and linking the website to that person based on the EVCG (formerly QCP-w)
QNCP-w	Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person based on the BRG
QSCD	Qualified electronic Signature/Seal Creation Device [eIDAS#AnnexII]
QTSP	Qualified TSP
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest-Shamir-Adleman (public-key cryptosystem, described by Ron Rivest, Adi Shamir and Leonard Adleman)
RSASSA	RSA Signature Scheme with Appendix
RSASSA-PSS	improved Probabilistic RSA Signature Scheme
SCT	Signed Certificate Timestamp
SHA	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extensions
SOG-IS	Senior Officials Group Information Systems Security
SSL	Secure Socket Layer
SÜG	Sicherheitsüberprüfungsgesetz
TLS	Transport Layer Security
TSP	Trust Service Provider
URL	Uniform Ressource Locator

UTC	Coordinated Universal Time
VDG	Vertrauensdienstegesetz
VDV	Vertrauensdiensteverordnung
VSA	Verschlusssachenanweisung
VS-NfD	Verschlusssache - Nur für den Dienstgebrauch

Anhang B: Referenzen

Tabelle 5 - Referenzen

[ADTL]	Adobe Approved Trust-List Tech. Requirements
[APRP]	Apple Root Certificate Programm
[APCT]	Apple's Certificate Transparency policy
[BR]	CAB-Forum Baseline Requirements
[CCADB]	CCADB Policy
[eIDAS]	eIDAS (Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates)
[ETS401]	ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETS411-1]	ETSI EN 319-411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETS411-2]	ETSI EN 319-411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETS412-1]	ETSI EN 319-412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[ETS412-2]	ETSI EN 319-412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[ETS412-3]	ETSI EN 319-412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[ETS412-4]	ETSI EN 319-412-4: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
[ETS412-5]	ETSI EN 319-412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[ETS312]	ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[ETS431-1]	ETSI TS 119 431-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
[ETS461]	ETSI TS 119 461: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
[RFC5753]	RFC 5753 Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)
[RFC3279]	RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC3647]	RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[RFC5280]	RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC6960]	RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
[RFC6962]	RFC 6962 Certificate Transparency
[RFC4055]	RFC 4055 Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[RFC5756]	RFC 5756 Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters
[RFC4491]	RFC 4491 Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile
[RFC5480]	RFC 5480 Elliptic Curve Cryptography Subject Public Key Information, March 2009
[RFC5758]	RFC 5758 Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA, January 2010
[RFC8692]	RFC 8692 Internet X.509 Public Key Infrastructure: Additional Algorithm Identifiers for RSASSA-PSS and ECDSA Using SHAKEs, December 2019
[RFC8813]	RFC 8813 Clarifications for Elliptic Curve Cryptography Subject Public Key Information
[RFC5019]	RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments
[RFC8823]	RFC 8823 Extensions to Automatic Certificate Management Environment for End-User S/MIME Certificates
[EVCG]	CAB-Forum Extended Validation Certificate Guidelines
[GCTP]	google chrome Certicate Transparency Policy
[GCRP]	Chromium Root Certificate Policy
[GGS]	Google G-Suite SMIME Zertifikatsprofil
[GCTL]	Google Certificate Transparency Log Policy
[MSRP]	Microsoft Trusted Root Program inkl. - Security Incident Response Requirements - Audit Requirements -Testing Instruction - New CA application
[MOZRP]	Mozilla Root Store Policy
[MOZCA]	Mozilla CA/Application Process
[NCSSR]	CAB-Forum Network Security Guidelines
[SÜG]	Sicherheitsüberprüfungsgesetz
[TR2102]	Technische Richtlinie TR-2102-1, Kryptographische Verfahren, Empfehlungen und Schlüssellängen, Bundesamt für die Sicherheit in der Informationstechnik
[TR3145]	Technische Richtlinie TR-03145-1, Secure CA operation, Part 1, Bundesamt für die Sicherheit in der Informationstechnik
[TR3145VS]	Technische Richtlinie TR-03145-VS-NfD, Secure CA operation, VS-NfD, Bundesamt für die Sicherheit in der Informationstechnik
[VDG]	Vertrauensdienstegesetz
[VDV]	Vertrauensdiensteverordnung
[VSA]	Verschlusssachenanweisung des Bundes
[X500]	ITU-T X.500 Serie / ISO/IEC 9594 Serie Information technology - Open systems interconnection - The Directory
[X509]	Recommendation ITU-T X.509 Information technology - Open Systems interconnection - The Directory: Public-key and attribute certificate frameworks

Anhang C: Definitionen

Hinweis: Es wird an dieser Stelle darauf verzichtet, bekannte Definitionen international etablierter Begriffe im PKI-Umfeld erneut aufzuführen, diesbezüglich sei auf die Definitionen der in Anhang B aufgeführten ETSI-Spezifikationen und RFCs verwiesen. Nachfolgend werden zum einen Begriffe definiert, die spezifisch für bestimmte Zertifikatstypen verwendet werden und zum anderen werden einige in diesem Dokument verwendete Begriffe klargestellt, deren Verwendung sich ggf. zwischen der deutschen und der englischen Sprache unterscheidet.

Tabelle 6 - Definitionen

Begriff	Bedeutung
Certification Authority Authorization (CAA)	DNS-Ressourceneintrag, der es dem Inhaber eines DNS-Domänen Namens ermöglicht, die TSP anzugeben, die berechtigt sind, Zertifikate für diese Domäne auszustellen
Fortgeschrittene elektronische Signatur	Elektronische Signatur nach [eIDAS#Art.26]
Fortgeschrittenes elektronisches Siegel	Elektronisches Siegel nach [eIDAS#Art.36]
High-Risk-Zertifikatsanträge	Zertifikatsanträge, welche die TSP anhand interner Kriterien für eine zusätzliche Prüfung kennzeichnen. Dazu können gehören: ▪ Domain Namen mit gemischten Zeichen (Mixed character domain names) ▪ Namen, bei denen ein höheres Risiko für Phishing oder andere betrügerische Nutzung besteht, ▪ Namen, die in zuvor abgelehnten Zertifikatsanträgen oder widerrufenen Zertifikaten enthalten sind, ▪ Namen, die auf der Miller Smiles Phishing-Liste oder der Google Safe Browsing-Liste aufgeführt sind, oder ▪ Namen, die ein TSP anhand ihrer eigenen Kriterien zur Risikominderung identifiziert
Interne Namen	Domain Namen, die nicht als global eindeutig im öffentlichen DNS verifiziert werden können, da sie nicht mit einer von der I-ANA registrierten Top Level Domain enden.
Kurzzeitzertifikat	Zertifikat, dessen Gültigkeitsdauer kürzer ist als die im CPS angegebene maximale Bearbeitungszeit für einen Sperrantrag
Leaf Zertifikat	Ein Zertifikat, dass zuvor als *Pre-Zertifikat* veröffentlicht wurde
Non-Reserved LDH-Label	Komponente eines Domain Namens, die kein '-' an der dritten und vierten Position hat
NULL-PIN-Status	Transportzustand einer noch nicht aktivierten TCOS-Smartcard mit nicht verwendbarer PIN.

P-Label	Komponente eines Domain Namens, die ein '-' an der dritten und vierten Position hat („XN-Label“) und auf die ab der fünften Position eine gültige Ausgabe des Punycode-Algorithmus gemäß [RFC3492# 6.3] folgt
Pre-Zertifikat	Zertifikat gemäß [RFC6962] zur öffentlichen Protokollierung eines noch auszustellenden Zertifikats. Das Pre-Zertifikat wird aus dem noch auszustellenden Zertifikat (exakte 1:1 Kopie) zzgl. der speziellen kritischen Erweiterung `Certificate Transparency precertificate poison extension (OID 1.3.6.1.4.1.11129.2.4.3)` erzeugt. Pre-Zertifikate gelten nicht als Zertifikat gemäß [RFC5280] und können von Standard-X.509v3-Clients nicht validiert werden. Das später aus dem Pre-Zertifikat erzeugte (echte) Zertifikat wird als *Leaf-Zertifikat* bezeichnet.
Pseudonym	Fiktive Identität, die eine Person zu einem bestimmten Zweck annimmt und die sich von ihrer ursprünglichen oder wahren Identität unterscheidet. HINWEIS: Eine pseudonyme Identität kann, im Gegensatz zu einer anonymen Identität, mit der wahren Identität der Person verknüpft werden. Die wahre Identität ist dem TSP bekannt.
Signed Certificate Timestamp (SCT)	Rückgabewert eines CT-Log-Servers gemäß [RFC6962] auf ein vom TSP dort veröffentlichtes Pre-Zertifikat. Alle auf die Veröffentlichung eines Pre-Zertifikates in verschiedenen CT-Log-Servern zurückgelieferten SCT werden in das Leaf-Zertifikat in die Erweiterung signedCertificateTimestampList aufgenommen.
Software-Zertifikat	Zertifikat zu einem Schlüsselpaar, welches mittels Krypto-Software auf einem Computer, nicht in einem kryptografischen Gerät (HSM, Smartcard) erzeugt wurde
Technisch beschränkte CA	Eine Sub-CA, bei der eine Kombination aus Werten in den Erweiterungen extendedKeyUsage und nameConstraints verwendet wird, um den Bereich zu begrenzen, in dem diese Sub-CA Endteilnehmer- oder weitere Sub-CA-Zertifikate ausstellen darf
Token	Hardware-Modul, das kryptografische Schlüssel auf sichere Weise erzeugt und/oder handhabt
Verifizierte Methode der Kommunikation	Kommunikation mit einer Person in einer Rolle eines Zertifikatsnehmers, die z. B. über eine postalische Anschrift, Telefonnummer oder E-Mail-Adresse erfolgt, welche über eine vom Zertifikatsnehmer unabhängige Quelle (QIIS, QGIS) ermittelt wurde
Verschlusssache - Nur für den Dienstgebrauch	Klassifizierung von zu schützenden staatlichen Informationen
Wildcard Zertifikat	Ein Zertifikat mit einem *Wildcard Domain Namen*
Wildcard Domain Name	Ein Domain Name, bestehend aus einem einzelnen Sternchen, gefolgt von einem einzelnen Punkt ("*."), gefolgt von einem voll qualifizierten Domänennamen

Anhang D: Zertifikatsprofile

Nachfolgend werden die obligatorischen und optionalen Erweiterungen und `subjectDN`-Attribute einzelner Zertifikatstypen aufgeführt. Dort nicht aufgeführte Erweiterungen und Attribute DÜRFEN NICHT gesetzt werden.

Anhang D1: Root-Zertifikate

Folgende Attribute des `subjectDN` MÜSSEN gesetzt werden:

- `commonName`
- `organizationName`
- `countryName`

Folgende Erweiterungen MÜSSEN gesetzt werden:

- `subjectKeyIdentifier`
- `keyUsage`
- `basicConstraints`

Folgende Erweiterung DARF gesetzt werden:

- `authorityKeyIdentifier`

Anhang D2: Sub-CA-Zertifikate

Folgende Attribute des `subjectDN` MÜSSEN gesetzt werden:

- `commonName`
- `organizationName`
- `countryName`

Folgende Erweiterungen MÜSSEN gesetzt werden:

- `subjectKeyIdentifier`
- `keyUsage`
- `basicConstraints`
- `authorityKeyIdentifier`
- [TLS] [SMIME] `certificatePolicies`
- [TLS] [SMIME] `extendedKeyUsage`
- [TLS] [SMIME] `cRLDistributionPoints`
- [TLS] [SMIME] `authorityInfoAccess`

Folgende Erweiterungen DRÜFEN gesetzt werden:

- `cRLDistributionPoints`
- `authorityInfoAccess`
- [QCP] `validityModel`

[TLS] [SMIME] Die o.g. Anforderungen gelten für Sub-CA Zertifikate. Bei Cross-Zertifikaten MÜSSEN die Anforderungen aus [BR] bzw. [SBR] berücksichtigt werden.

Anhang D3: OCSP-Signer-Zertifikate

Folgende Erweiterungen MÜSSEN gesetzt werden:

- `authorityKeyIdentifier`
- `keyUsage`
- `extendedKeyUsage`

Folgende Erweiterungen DÜRFEN gesetzt werden:

- `basicConstraints`
- `subjectKeyIdentifier`
- `signedCertificateTimestampList`

Bzgl. der Verwendung der Erweiterungen `id-pkix-ocsp-nocheck`, `cRLDistribution-Points` und `authorityInfoAccess` zur Überprüfung der OCSP-Signer-Zertifikate siehe Kap. 7.3.

Folgende Attribute des `subjectDN` MÜSSEN gesetzt werden:

- `commonName`
- `countryName`
- `organizationName`

Anhang D4: Endteilnehmer-Zertifikate

Anhang D4.1: TLS-Zertifikate

[TLS] Folgende Erweiterungen MÜSSEN gesetzt werden:

- `authorityKeyIdentifier`
- `keyUsage`
- `certificatePolicies`
- `subjectAltName`
- `extendedKeyUsage`
- `cRLDistributionPoints`
- `authorityInfoAccess`
- `signedCertificateTimestampList`

Folgende Erweiterungen DÜRFEN gesetzt werden:

- `subjectKeyIdentifier`
- `basicConstraints`

[EVCP] Ergänzend zu [TLS] MUSS die Erweiterung `CABFOrganizationIdentifier` gesetzt werden, wenn der `organizationIdentifier` gesetzt ist, ansonsten DARF sie gesetzt werden.

[QEVCP-w] Ergänzend zu [TLS] und [EVCP] MUSS die Erweiterung `qcStatements` gesetzt werden.

[DVCP] Folgendes Attribut des `subjectDN` MUSS gesetzt werden:

- `commonName`

[OVCP] Folgende Attribute des `subjectDN` MÜSSEN gesetzt werden:

- `commonName`
- `countryName`
- `stateOrProvinceName`, wenn `localityName` nicht gesetzt wird
- `localityName`, wenn `stateOrProvinceName` nicht gesetzt wird
- `organizationName`

Folgende Attribute des `subjectDN` DÜRFEN gesetzt werden:

- `countryName`
- `postalCode`
- `streetAddress`
- `stateOrProvinceName`
- `localityName`

[EVCP] Ergänzend zu [OVCP] gelten folgende Anforderungen:

Folgende Attribute des `subjectDN` MÜSSEN gesetzt werden:

- `businessCategory`
- `jurisdictionOfIncorporationCountryName`
- `jurisdictionOfIncorporationStateOrProvinceName`, wenn die Registrierungsinstanz auf Ebene eines Bundeslands oder auf kommunaler Ebene agiert, ansonsten DARF er NICHT gesetzt werden.
- `jurisdictionLocalityName`, wenn die Registrierungsinstanz auf kommunaler Ebene agiert, ansonsten DARF er NICHT gesetzt werden.
- `serialNumber`

Folgendes Attribut des `subjectDN` DARF gesetzt werden:

- `organizationIdentifier`

Anhang D4.2: S/MIME-Zertifikate

[SMIME] Folgende Erweiterungen MÜSSEN gesetzt werden:

- `certificatePolicies`
- `cRLDistributionPoints`
- `authorityInformationAccess`
- `keyUsage`
- `extKeyUsage`
- `authorityKeyIdentifier`
- `subjectAlternativeName`
- `subjectKeyIdentifier`
- [QCP] `qcStatements`

Folgende Erweiterung DARF gesetzt werden:

- `basicConstraints`

[SMV] Folgendes Attribut des `subjectDN` MUSS gesetzt werden:

- `commonName`

Folgende Attribute des `subjectDN` DÜRFEN gesetzt werden:

- `serialNumber`
- `emailAddress`

[SOV] Folgende Attribute des `subjectDN` MÜSSEN gesetzt werden:

- `commonName`
- `organizationName`
- `organizationIdentifier`
- `countryName`

Folgende Attribute des `subjectDN` DÜRFEN gesetzt werden:

- `organizationalUnitName`
- `serialNumber`
- `emailAddress`
- `localityName`
- `stateOrProvinceName`
- [Legacy, Multipurpose] `streetAddress`
- [Legacy, Multipurpose] `postalCode`

[SSV] Folgende Attribute des `subjectDN` MÜSSEN gesetzt werden:

- `commonName`
- `organizationName`
- `organizationIdentifier`
- `surname und givenName oder pseudonym`
- `countryName`

Folgende Attribute des `subjectDN` DÜRFEN gesetzt werden:

- `serialNumber`
- `emailAddress`
- `title`
- `localityName`
- `stateOrProvinceName`
- [Legacy] [Multipurpose] `streetAddress`
- [Legacy] [Multipurpose] `postalCode`

[SIV] Folgende Attribute des `subjectDN` MÜSSEN gesetzt werden:

- `commonName`
- `surname und givenName oder pseudonym`
- `countryName`

Folgende Attribute des `subjectDN` DÜRFEN gesetzt werden:

- `serialNumber`
- `emailAddress`
- `title`
- `localityName`
- `stateOrProvinceName`
- [Legacy] [Multipurpose] `streetAddress`
- [Legacy] [Multipurpose] `postalCode`

Anhang D4.3: Generische Zertifikatsprofile gemäß ETSI

[ETSI] Folgende Erweiterungen MÜSSEN in Zertifikaten für natürliche Personen oder Organisationen mindestens gesetzt werden:

- `authorityKeyIdentifier`
- `keyUsage`
- `certificatePolicies`
- `authorityInfoAccess`
- ggf. `cRLDistributionPoints` (siehe Kap. 7.1.2 (31))
- [QCP] `qcStatement`

Darüber hinaus DÜRFEN die in Tabelle 2 aufgeführten Erweiterungen gesetzt werden.

[ETSI] Folgende Attribute des `subjectDN` MÜSSEN in Zertifikaten für natürliche Personen, die nicht in Verbindung mit einer Organisation stehen, gesetzt werden:

- `countryName`
- `commonName`
- `surname und givenName` oder `pseudonym`
- `serialNumber`, sofern die weiteren Attribute des `subjectDN` keine Eindeutigkeit sicherstellen

Darüber hinaus DÜRFEN die in Tabelle 3 aufgeführten Attribute gesetzt werden, die sich nicht auf Organisation beziehen.

[ETSI] Folgende Attribute des `subjectDN` MÜSSEN in Zertifikaten für natürliche Personen, die in Verbindung zu einer Organisation stehen gesetzt werden:

- `countryName`
- `commonName`
- `surname und givenName oder pseudonym`
- `organizationName`
- `serialNumber`, sofern die weiteren Attribute des `subjectDN` keine Eindeutigkeit sicherstellen

Darüber hinaus DÜRFEN die in Tabelle 3 aufgeführten Attribute gesetzt werden.

[ETSI] Folgende Attribute des `subjectDN` MÜSSEN in Zertifikaten für Organisationen gesetzt werden:

- `countryName`
- `organizationName`
- `organizationIdentifier`
- `commonName`

Darüber hinaus DÜRFEN die in Tabelle 3 aufgeführten Attribute gesetzt werden, die sich nicht auf natürliche Personen beziehen.

Anhang D4.4: Zertifikatsprofile gemäß [3145]

Für die Zertifikate nach [TR3145] gibt es nur wenige generische Vorgaben, so dass an dieser Stelle keine generischen oder konkreten Zertifikatsprofile aufgeführt werden.

Die Zertifikatsprofile MÜSSEN in den CPS beschrieben werden.