Deutsche Telekom Security GmbH

Trust Center Certificate Policy

Version 10.0 (**final**)
17.11.2026



Change history | Änderungshistorie

Table 1 – Change history | Tabelle 2 – Änderungshistorie

Version	Date | Stand	Changes | Änderungen
1	2021-03-15	Initial version based on | 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
2	2022-03-02	Annual review, upates | Jährliches Review, Aktualisierungen: [BR] 1.7.4 – 1.8.1, [NCSSR] 1.6 - 1.7, [EVCG] 1.7.5 - 1.7.8, [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, [ETS411-2] 2.4.1, [ETS412-4] 1.2.1
3	2023-01-24	Annual review, upates | Jährliches Review, Aktualisierungen: [BR] 1.8.2 – 1.8.6, [EVCG] 1.7.9 – 1.8.0
4	2023-09-01	Inclusion | Aufnahme: [SBR] 1.0.0, [ETS411-6] 1.1.1 Updates | Aktualsisierungen: [BR] 1.8.7 – 2.0.0
5	2024-08-30	Annual review, cleanup | Jährliches Review, Bereinigung Merging the English and German versions | Zusammenführung der englischen und der deutschen Fassung Upates | Aktualisierungen: [BR] 2.0.1 – 2.0.5, [NCSSR] 2.0, [SBR] 1.0.1 - 1.0.4, [EVCG] 1.8.1 – 2.0.1, [ETS401] 3.1.1, [ETS411-1] 1.4.1, [ETS411-2] 2.5.1, [ETS412-1] 1.5.1, [ETS412-2] 2.3.1, [ETS412-3] 1.3.1, [ETS412-4] 1.3.1, [ETS412-5] 2.4.1, [ETS312] 1.4.3
6	2025-01-15	Upates | Aktualisierungen: [BR] 2.0.6 – 2.1.2, [SBR] 1.0.5 - 1.0.8, [ETS412-4] 1.3.2, [ETS312] 1.5.1
7	2025-07-05	Upates | Aktualisierungen: New Policies QCP-l, QCP-n, QNCP-w | Neue Policies QCP-l, QCP-n, QNCP-w
8	2025-12-01	Upates | Aktualisierungen: [BR] 2.1.3 – 2.1.9, [SBR] 1.0.9 - 1.0.12, [ETS411-1] 1.5.1, [ETS411-2] 2.6.1, [ETS412-1] 1.6.1, [ETS412-2] 2.4.1, [ETS412-4] 1.4.1, [ETS412-5] 2.5.1, [NCSSR] 2.0.1 - 2.0.5
9	2026-03-15	Upates | Aktualisierungen: [BR] 2.2.0 – 2.2.5, [SBR] 1.0.13
10	2026-11-17	Upates | Aktualisierungen: new variant of the organizationIdentifier included | neue Variante des organizationIdentifiers aufgenommen

This work is licensed under | Dieses Dokument ist lizenziert unter
Creative Commons Attribution - NoDerivatives 4.0 International License
(https://creativecommons.org/licenses/by-nd/4.0/) .

Copyright © 2026 Deutsche Telekom Security GmbH, Bonn

Contents | Inhalt

List of tables | Tabellenverzeichnis 9

1 Introduction | Einleitung 10

1.1 Overview | Überblick 10

1.2 Document name and identification | Name und Kennzeichnung des Dokuments 13

1.3 PKI participants | PKI-Teilnehmer 13
1.3.1 Certification Authorities | Zertifizierungsstellen 13
1.3.2 Registration Authorities | Registrierungsstellen 14
1.3.3 Subscribers | Zertifikatsnehmer 15
1.3.4 Relying parties | Zertifikatsnutzer (vertrauende Dritte) 16
1.3.5 Other participants | Andere Teilnehmer 16

1.4 Certificate usage | Zertifikatsverwendung 16
1.4.1 Appropriate certificate uses | Zulässige Verwendung von Zertifikaten 17
1.4.2 Prohibited certificate uses | Unzulässige Verwendung von Zertifikaten 17

1.5 Policy administration | Verwaltung des Dokuments 17
1.5.1 Organization administering the document | Verwaltende Organisation dieses Dokuments 17
1.5.2 Contact person | Ansprechpartner 17
1.5.3 Person determining CPS suitability for the policy | Instanz für die Feststellung der Konformität eines CPS zu dieser CP 17
1.5.4 CPS approval procedures | Genehmigungsverfahren dieser CP und eines CPS 18

1.6 Definitions and acronyms | Definitionen und Abkürzungen 18

2 Publication and repository responsibilities | Verantwortung für Veröffentlichung und Verzeichnisse 19

2.1 Repositories | Verzeichnisse 19

2.2 Publication of certification information | Veröffentlichung von Informationen zu Zertifikaten 19

2.3 Time or frequency of publication | Zeitpunkt oder Häufigkeit von Veröffentlichungen 20

2.4 Access controls on repositories 21

3 Identification and Authentication | Identifzierung und Authentifizierung 22

3.1 Naming | Namensregeln 22
3.1.1 Types of names | Namensformen 22
3.1.2 Need for names to be meaningful | Aussagekraft von Namen 22
3.1.3 Anonymity or pseudonymity of subscribers | Anonymität bzw. Pseudonyme der Zertifikatsnehmer 23
3.1.4 Rules for interpreting various name forms | Regeln zur Interpretation verschiedener Namensformen 23
3.1.5 Uniqueness of names | Eindeutigkeit von Namen 23
3.1.6 Recognition, authentication, and role of trademarks | Erkennung, Authentifizierung und Rolle von Markennamen 24

3.2 Initial identity validation | Initiale Validierung der Identität 24
3.2.1 Method to prove possession of private key | Methoden des Besitznachweises des privaten Schlüssels 24
3.2.2 Authentication of organization identity | Authentifizierung der Identität von Organisationen 24
3.2.3 Authentication of individual identity | Authentifizierung der Identität natürlicher Personen 26
3.2.4 Non-verified subscriber information | Nicht überprüfte Informationen 27
3.2.5 Validation of authority | Validierung der Bevollmächtigung 27
3.2.6 Criteria for interoperation | Kriterien für Interoperabilität 28
3.2.7 Validation of control over a domain or IP-address | Validierung der Kontrolle über eine Domain oder IP-Adresse 28
3.2.8 Validation of control over an email address | Validierung der Kontrolle über eine E-Mail-Adresse 29

3.3 Identification and authentication for re-key requests | Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung 30
3.3.1 Identification and authentication for routine re-key | Identifizierung und Authentifizierung für routinemäßige Schlüsselerneuerung 30
3.3.2 Identification and authentication for re-key after revocation | Identifizierung und Authentifizierung für Schlüsselerneuerung nach einer Sperrung 30

3.4 Identification and authentication for revocation request | Identifizierung und Authentifizierung von Sperranträgen 30

4 Certificate Life-cycle operational requirements | Betriebliche Anforderungen an den Zertifikats-Lebenszyklus 31

4.1 Certificate Application | Zertifikatsantrag *31*
4.1.1 Who can submit a certificate application? | Zertifikatsantragsberechtigte 31
4.1.2 Enrollment process and responsibilities | Antragsprozess und -verantwortlichkeiten 31

4.2 Certificate application processing | Bearbeitung der Zertifikatsanträge *32*
4.2.1 Performing identification and authentication functions | Durchführung der Identifizierung und Authentifizierung 33
4.2.2 Approval or rejection of certificate applications | Genehmigung oder Ablehnung von Zertifikatsanträgen 35
4.2.3 Time to process certificate applications | Fristen für die Bearbeitung von Zertifikatsanträgen 36

4.3 Certificate issuance | Zertifikatsausstellung *37*
4.3.1 CA actions during certificate issuance | TSP-Aktivitäten während der Zertifikatsaustellung 37
4.3.1.1 CA certificate issuance | Ausstellung von CA-Zertifikaten 37
4.3.1.2 Subscriber certificate issuance | Ausstellung von Endteilnehmer-Zertifikaten 38
4.3.2 Notification to subscriber by the CA of issuance of certificate | Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines Zertifikats 38

4.4 Certificate acceptance | Zertifikatsannahme *39*
4.4.1 Conduct constituting certificate acceptance | Verhalten, das die Annahme eines Zertifikats bestätigt 39
4.4.2 Publication of the certificate by the CA 39
4.4.3 Notification of certificate issuance by the CA to other entities 39

4.5 Key pair and certificate usage | Schlüssel- und Zertifikatsnutzung *39*
4.5.1 Private key and certificate usage | Nutzung des privaten Schlüssels und des Zertifikats 39
4.5.2 Relying party public key and certificate usage | Nutzung des öffentlichen Schlüssels und des Zertifikats durch Dritte 39

4.6 Certificate renewal | Zertifikatserneuerung unter Beibehaltung der Schlüssel *39*
4.6.1 Circumstance for certificate renewal | Umstände für ein Renewal 39
4.6.2 Who may request renewal | Antragsberechtigte für ein Renewal 40
4.6.3 Processing certificate renewal requests | Verarbeitung von Anträgen auf Renewal 40
4.6.4 Notification of new certificate issuance to subscriber | Benachrichtigung des Zertifikatsnehmers über die Ausstellung neuer Zertifikate 40
4.6.5 Conduct constituting acceptance of a renewal certificate | Verhalten, das die Annahme eines erneuerten Zertifikats bestätigt 40
4.6.6 Publication of the renewal certificate by the CA | Veröffentlichung erneuerter Zertifikate durch die TSP 40
4.6.7 Notification of certificate issuance by the CA to other entities | Information Dritter über die Ausstellung neuer Zertifikate durch die TSP 40

4.7 Certificate re-key | Zertifikatserneuerung mit neuen Schlüsseln *41*
4.7.1 Circumstance for certificate re-key | Umstände für eine Schlüsselerneuerung 41
4.7.2 Who may request certification of a new public key | Antragsberechtigte für eine Schlüsselerneuerung 41
4.7.3 Processing certificate re-keying requests | Verarbeitung von Anträgen auf Schlüsselerneuerung 41
4.7.4 Notification of new certificate issuance to subscriber | Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines erneuerten Zertifikats 41
4.7.5 Conduct constituting acceptance of a re-keyed certificate | Verhalten, das die Annahme eines erneuerten Zertifikats bestätigt 41
4.7.6 Publication of the re-keyed certificate by the CA | Veröffentlichung erneuerter Zertifikate durch die TSP 42
4.7.7 Notification of certificate issuance by the CA to other entities | Information Dritter über die Ausstellung neuer Zertifikate durch den TSP 42

4.8 Certificate modification | Änderung von Zertifikatsdaten *42*
4.8.1 Circumstance for certificate modification | Umstände für eine Änderung von Zertifikatsdaten 42
4.8.2 Who may request certificate modification 42
4.8.3 Processing certificate modification requests 42
4.8.4 Notification of new certificate issuance to subscriber 43
4.8.5 Conduct constituting acceptance of modified certificate 43
4.8.6 Publication of the modified certificate by the CA 43
4.8.7 Notification of certificate issuance by the CA to other entities 43

4.9 Certificate revocation and suspension | Zertifikatssperrung und Suspendierung *43*
4.9.1 Circumstances for revocation | Sperrgründe 43
4.9.1.1 Reasons for revoking a Sub CA certificate | Gründe für die Sperrung eines Sub-CA Zertifikats 43
4.9.1.2 Reasons for revoking a subscriber certificate | Gründe für die Sperrung eines Endteilnehmer-Zertifikats 44
4.9.2 Who can request revocation | Berechtigte Sperrantragsteller 46
4.9.3 Procedure for revocation request | Ablauf einer Sperrung 47
4.9.4 Revocation request grace period | Fristen zur Beantragung einer Sperrung 47
4.9.5 Time within which CA must process the revocation request | Fristen zur Verarbeitung von Sperranträgen durch die TSP .47
4.9.6 Revocation checking requirement for relying parties | Anforderungen an Zertifikatsnutzer zur Prüfung von Sperrinformationen 49
4.9.7 CRL issuance frequency 49

4.9.8 Maximum latency for CRLs | Maximale Latenzzeit von Sperrlisten 50
4.9.9 On-line revocation/status checking availability | Verfügbarkeit von Online-Sperr-/Statusinformationen 50
4.9.10 On-line revocation checking requirements | Anforderungen an Online-Überprüfungsverfahren 50
4.9.11 Other forms of revocation advertisements available | Andere verfügbare Formen der Bekanntmachung von Sperrinformationen 50
4.9.12 Special requirements related to key compromise | Gesonderte Bedingungen bei Kompromittierung privater Schlüssel 50
4.9.13 Circumstances for suspension | Umstände für eine Suspendierung 50
4.9.14 Who can request suspension | Berechtigte Antragsteller für eine Suspendierung 51
4.9.15 Procedure for suspension request | Ablauf einer Suspendierung 51
4.9.16 Limits on suspension period | Begrenzung der Suspendierungsperiode 51

4.10 Certificate status services | Zertifikatsstatusdienste 51
4.10.1 Operational characteristics | Betriebliche Vorgaben 51
4.10.1.1 Operational characteristics for the provision of the OCSP responder | Betriebliche Vorgaben für die Bereitstellung der OCSP-Responder 52
4.10.1.2 Operational characteristics for the provision of revocation lists | Betriebliche Vorgaben für die Bereitstellung der Sperrlisten 53
4.10.2 Service availability | Verfügbarkeit 53
4.10.3 Optional features | Optionale Merkmale 53

4.11 End of subscription | Kündigung durch den Zertifikatsnehmer 53

4.12 Key escrow and recovery | Schlüsselhinterlegung und Wiederherstellung 54
4.12.1 Key escrow and recovery policy and practices | Schlüsselhinterlegungs- und Wiederherstellungsrichtlinien und -Praktiken 54
4.12.2 Session key encapsulation and recovery policy and practices | Richtlinien und Praktiken zur Kapselung und Wiederherstellung von Sitzungsschlüsseln 54

5 Facility, Management an operational controls | Bauliche, organistaorische und betriebliche Regelungen 55

5.1 Physical controls | Physikalische Maßnahmen 56
5.1.1 Site location and construction | Standort und Bauweise 57
5.1.2 Physical access | Physikalischer Zutritt 57
5.1.3 Power and air conditioning | Stromversorgung und Klimatisierung 57
5.1.4 Water exposures | Wassereinwirkung 58
5.1.5 Fire prevention and protection | Brandvorsorge und Brandschutz 58
5.1.6 Media storage | Aufbewahrung von Medien 58
5.1.7 Waste disposal | Abfallentsorgung 58
5.1.8 Off-site backup | Externe Sicherung 58

5.2 Procedural controls | Organisatorische Maßnahmen 58
5.2.1 Trusted roles | Vertrauenswürdige Rollen 58
5.2.2 Number of persons required per task | Anzahl der für eine Aufgabe erforderlichen Personen 59
5.2.3 Identification and authentication for each role | Identifizierung und Authentifizierung für vertrauenswürdige Rollen 60
5.2.4 Roles requiring separation of duties | Rollen, die eine Aufgabentrennung erfordern 61

5.3 Personnel controls | Personelle Maßnahmen 61
5.3.1 Qualifications, experience, and clearance requirements | Qualifikationen, Erfahrung und Freigaben 61
5.3.2 Background check procedures | Verfahren zur Hintergrundprüfung 62
5.3.3 Training requirements | Schulungsanforderungen 62
5.3.4 Retraining frequency and requirements | Nachschulungsintervalle und -anforderungen 63
5.3.5 Job rotation frequency and sequence | Häufigkeit und Abfolge der Arbeitsplatzrotation 63
5.3.6 Sanctions for unauthorized actions | Sanktionen bei unbefugten Handlungen 63
5.3.7 Independent contractor requirements | Anforderungen an unabhängige Auftragnehmer 63
5.3.8 Documentation supplied to personnel | Dem Personal bereit gestellte Dokumentation 63

5.4 Audit logging procedures | Protokollierungsverfahren 64
5.4.1 Types of events recorded | Zu protokollierende Ereignisse 64
5.4.2 Frequency of processing log | Häufigkeit der Log-Verarbeitung 64
5.4.3 Retention period for audit log | Aufbewahrungszeitraum für Logdaten 64
5.4.4 Protection of audit log | Schutz der Audit-Protokolle 65
5.4.5 Audit log backup procedures | Backup-Verfahren für Audit-Protokolle 65
5.4.6 Audit collection system (internal vs. external) | Audit-Sammelsystem (intern vs. extern) 65
5.4.7 Notification to event-causing subject | Benachrichtigung der Person, die ein Ereignis ausgelöst hat 65
5.4.8 Vulnerability assessments | Nutzung von Protokolldaten zur Schwachstellenprüfung 65

5.5 Records archival | Aufbewahrung von Aufzeichnungen 65
5.5.1 Types of records archived | Aufzubewahrende Aufzeichnungen 66

5.5.2 Retention period for archive | Aufbewahrungszeitraum für Aufzeichnungen 67
5.5.3 Protection of archive | Schutz der Aufzeichnungen 67
5.5.4 Archive backup procedures | Backup-Verfahren für Aufzeichnungen 68
5.5.5 Requirements for timestamping of records | Anforderungen an Zeitstempel von Datensätzen 68
5.5.6 Archive collection system (internal or external) | Archivsystem (intern oder extern) 68
5.5.7 Procedures to obtain and verify archive information | Verfahren zur Beschaffung und Überprüfung von Aufzeichnungen 68

5.6 Key changeover | Schlüsselwechsel 68

5.7 Compromise and disaster recovery | Kompromittierung und Notfall-Wiederherstellung 69
5.7.1 Incident and compromise handling procedures | Verfahren zur Meldung und Behandlung von Vorfällen und Kompromittierungen 69
5.7.2 Computing resources, software, and/or data are corrupted | Wiederherstellung bei Beschädigung von Computern, Software oder Daten 70
5.7.3 Entity private key compromise procedures | Verfahren bei Kompromittierung von privaten Schlüsseln 70
5.7.4 Business continuity capabilities after a disaster 71

5.8 CA or RA termination 71

6 Technical security controls | Technische Sicherheitsmaßnahmen 73

6.1 Key pair generation and installation | Generierung und Installation von Schlüsselpaaren 73
6.1.1 Key pair generation | Generierung von Schlüsselpaaren 73
6.1.1.1 Generierung von CA-Schlüsselpaaren 73
6.1.1.2 Generierung von OCSP-Signer-Schlüsselpaaren 74
6.1.1.3 Generierung von RA-Schlüsselpaaren 74
6.1.1.4 Generierung von Endteilnehmer-Schlüsselpaaren 74
6.1.2 Private key delivery to subscriber | Bereitstellung der privaten Schlüssel an die Zertifikatsnehmer 75
6.1.3 Public key delivery to certificate issuer | Übergabe öffentlicher Schlüssel an die TSP 75
6.1.4 CA public key delivery to relying parties | Bereitstellung der öffentlichen CA-Schlüssel 76
6.1.5 Key sizes | Schlüssellängen 76
6.1.6 Public key parameters generation and quality checking | Generierung und Qualitätsprüfung öffentlicher Schlüsselparameter 77
6.1.7 Key usage purposes | Schlüsselverwendung 77

6.2 Private Key Protection and Cryptographic Module Engineering Controls | Schutz privater Schlüssel und technische Kontrollen kryptografischer Module 78
6.2.1 Cryptographic module standards and controls | Standards und Kontrollen für kryptografische Module 78
6.2.2 Private key (n out of m) multi-person control | Mehrpersonenkontrolle über private Schlüssel (n von m) 78
6.2.3 Private key escrow | Hinterlegung privater Schlüssel 78
6.2.4 Private key backup | Sicherung privater Schlüssel 79
6.2.5 Private key archival | Archivierung privater Schlüssel 79
6.2.6 Private key transfer into or from a cryptographic module | Übertragung privater Schlüssel in oder von einem kryptografischen Modul 80
6.2.7 Private key storage on cryptographic module | Speicherung privater Schlüssel in kryptografischen Modulen 80
6.2.8 Method of activating private key | Methoden zur Aktivierung privater Schlüssel 80
6.2.9 Method of deactivating private key | Methoden zur Deaktivierung privater Schlüssel 81
6.2.10 Method of destroying private key | Methoden zur Zerstörung privater Schlüssel 81
6.2.11 Cryptographic Module Rating | Bewertung kryptografischer Module 81

6.3 Other aspects of key pair management | Andere Aspekte zur Verwaltung von Schlüsselpaaren 81
6.3.1 Public key archival | Archivierung des öffentlichen Schlüssels 81
6.3.2 Certificate operational periods and key pair usage periods | Nutzungsdauer von Zertifikaten und Schlüsselpaaren 81

6.4 Activation data | Aktivierungsdaten 82
6.4.1 Activation data generation and installation | Generierung und Installation von Aktivierungsdaten 82
6.4.2 Activation data protection | Schutz der Aktivierungsdaten 82
6.4.3 Other aspects of activation data | Andere Aspekte der Aktivierungsdaten 83

6.5 Computer security controls | Computer-Sicherheitsmaßnahmen 83
6.5.1 Specific computer security technical requirements | Spezifische technische Anforderungen an die Computersicherheit. 83
6.5.2 Computer security rating | Sicherheitsbewertung von Computern 85

6.6 Life cycle technical controls | Technische Kontrollen des Lebenszyklus 85
6.6.1 System development controls | Steuerung der Systementwicklung 86
6.6.2 Security management controls | Maßnahmen des Sicherheitsmanagements 86
6.6.3 Life cycle security controls | Sicherheitsmaßnahmen während des Lebenszyklus 87

6.7 Network security controls | Netzwerk-Sicherheitsmaßnahmen 87

6.8 Timestamping | Zeitstempel 89

7 Certifcate, CRL and OCSP Profiles | Zertifikats-, Sperrlisten- und OCSP-Profile 90

7.1 Certificate profiles | Zertifikatsprofile 90
7.1.1 Version number | Versionsnummer 90
7.1.2 Certificate extensions | Zertifikatserweiterungen 90
7.1.3 Algorithm object identifiers | Algorithmen-OID 96
7.1.4 Name forms | Namensformen 97
7.1.5 Name constraints 100
7.1.6 `certificatePolicies` object identifier | OIDs der Erweiterung `certificatePolicies` 100
7.1.7 Usage of `policyConstraints` extension | Verwendung der Erweiterung `policyConstraints` 101
7.1.8 `policyQualifiers` syntax and semantics | Syntax und Semantik der `policyQualifier` 101
7.1.9 Processing semantics for `certificatePolicies` | Verarbeitungssemantik für `certificatePolicies` 101

7.2 CRL profile | Sperrlistenprofile 101
7.2.1 Version number | Versionsnummer 101
7.2.2 CRL and CRL entry extensions 101

7.3 OCSP Profile | OCSP-Profil 102
7.3.1 Version number | Versionsnummer 102
7.3.2 OCSP extensions | OCSP Erweiterungen 103

8 Compliance audit and other assessments | Audits und andere Bewertungskriterien 104

8.1 Frequency or circumstances of assessment | Häufigkeit und Art der Prüfungen 104
8.1.1 Internal audits | Selbstüberprüfung 104
8.1.2 External Audits | Prüfungen durch externe Auditoren 104
8.1.3 Audits of subcontractors and delegated third parties | Prüfungen von Unterauftragnehmern und delegierten Dritten ... 104

8.2 Identity/qualifications of assessor | Identität/Qualifikation der Prüfer 105

8.3 Assessor's relationship to assessed entity | Beziehung des Prüfers zur geprüften Stelle 106

8.4 Topics covered by assessment | Abgedeckte Bereiche der Prüfung 106

8.5 Actions taken as a result of deficiency | Maßnahmen infolge von Mängeln 106

8.6 Communication of results | Mitteilung der Ergebnisse 107

9 Other Business and legal matters | Sonstige geschäftliche und rechtliche Bestimmungen 108

9.1 Fees | Entgelte 108
9.1.1 Certificate issuance or renewal fees | Gebühren für die Ausstellung oder Erneuerung von Zertifikaten 108
9.1.2 Certificate access fees | Gebühren für den Zertifikatszugang 108
9.1.3 Revocation or status information access fees | Gebühren für den Zugang zu Sperr- oder Statusinformationen 108
9.1.4 Fees for other services | Gebühren für andere Dienstleistungen 108
9.1.5 Refund policy | Rückerstattungsrichtlinie 108

9.2 Financial responsibility | Finanzielle Verantwortlichkeiten 108
9.2.1 Insurance coverage 109
9.2.2 Other assets | Sonstige Vermögensgegenstände 109
9.2.3 Insurance or warranty coverage for end entities | Versicherungs- oder Garantiedeckung für Endteilnehmer 109

9.3 Confidentiality of business information | Vertraulichkeit von Geschäftsinformationen 109
9.3.1 Scope of confidential information | Umfang an vertraulichen Informationen 109
9.3.2 Information not within the scope of confidential information | Umfang an nicht vertraulichen Informationen 110
9.3.3 Responsibility to protect confidential information | Verantwortung zum Schutz vertraulicher Informationen 110

9.4 Privacy of personal information | Schutz von personenbezogenen Daten 110
9.4.1 Privacy plan | Datenschutzkonzept 110
9.4.2 Information treated as private | Als privat zu behandelnde Informationen 110
9.4.3 Information not deemed private | Nicht als privat geltende Informationen 111
9.4.4 Responsibility to protect private information | Verantwortung für den Schutz privater Informationen 111
9.4.5 Notice and consent to use private information | Benachrichtigung und Zustimmung zur Verwendung privater Informationen 111
9.4.6 Disclosure pursuant to judicial or administrative process | Offenlegung im Rahmen eines Gerichts- oder Verwaltungsverfahrens 111
9.4.7 Other information disclosure circumstances | Andere Umstände der Offenlegung von Informationen 111

9.5 Intellectual property rights | Urheberrecht 111

9.6 Representations and warranties | Zusicherungen und Gewährleistungen 111
9.6.1 CA representations and warranties | Zusicherungen und Gewährleistungen der TSP 111

9.6.2 RA representations and warranties | Zusicherungen und Gewährleistungen der RAs ... 114
9.6.3 Subscriber representations and warranties | Zusicherungen und Gewährleistungen der Zertifikatsnehmer ... 114
9.6.4 Relying party representations and warranties | Zusicherungen und Gewährleistungen der Zertifikatsnutzer ... 117
9.6.5 Representations and warranties of other participants | Zusicherungen und Gewährleistungen sonstiger Teilnehmer ... 118
9.7 Disclaimers of warranties | Gewährleistungsausschlüsse ... 118
9.8 Limitations of liability | Haftungsbeschränkungen ... 118
9.9 Indemnities | Schadensersatz ... 118
9.10 Term and termination of this CP or a CPS | Laufzeit und Aufhebung dieser CP oder eines CPS ... 118
9.10.1 Term | Laufzeit ... 118
9.10.2 Termination | Aufhebung ... 119
9.10.3 Effect of termination and survival | Auswirkungen der Beendigung und Fortführung ... 119
9.11 Individual notices and communications with participants | Individuelle Mitteilungen und Kommunikation mit Teilnehmern ... 119
9.12 Amendments to this CP or a CPS | Änderungen an dieser CP oder einem CPS ... 119
9.12.1 Procedure for amendment | Verfahren für Änderungen ... 119
9.12.2 Notification mechanism and period | Benachrichtigungsmechanismus und -zeitraum ... 120
9.12.3 Circumstances under which OID must be changed | Umstände, unter denen die OID geändert werden muss ... 120
9.13 Dispute resolution provisions | Bestimmungen zur Beilegung von Streitigkeiten ... 120
9.14 Governing law | Geltendes Recht ... 120
9.15 Compliance with applicable law | Einhaltung geltenden Rechts ... 121
9.16 Miscellaneous provisions | Verschiedene Bestimmungen ... 121
9.16.1 Entire agreement | Gesamte Vereinbarung ... 121
9.16.2 Assignment | Zuordnung ... 121
9.16.3 Severability | Salvatorische Klausel ... 121
9.16.4 Enforcement (attorneys' fees and waiver of rights) | Rechtsdurchsetzung ... 121
9.16.5 Force Majeure | Höhere Gewalt ... 122
9.17 Other provisions | Sonstige Bestimmungen ... 122

Appendix | Anhang ... 123

Appendix A: Abbreviations | Anhang A: Abkürzungen ... 123

Appendix B: References | Anhang B: Referenzen ... 125

Appendix C: Definitions | Anhang C: Definitionen ... 127

Appendix D: Certificate Profiles | Anhang D: Zertifikatsprofile ... 130

D1: Root Certificates | Root-CA-Zertifikate ... 130

D2: Sub-CA Certificates | Sub-CA-Zertifikate ... 130

D3: OCSP-Signer Certificates | OCSP-Signer-Zertifikate ... 131

D4: Subscriber Certificates | Endteilnehmer-Zertifikate ... 131

D4.1: TLS Certificates | TLS-Zertifikate ... 132

D4.2: S/MIME Certificates | S/MIME-Zertifikate ... 133

D4.3: Generic Certificate Profiles according to ETSI | Generische Zertifikatsprofile gemäß ETSI ... 134

List of tables | Tabellenverzeichnis

Table 1 – Change history | Tabelle 2 – Änderungshistorie 2

Table 2 – Certficate Extensions | Tabelle 2 – Zertifikatserweiterungen 91

Table 3 – Name forms | Tabelle 3 – Namensformen 98

Table 4 – Abbreviations | Tabelle 4 – Abkürzungen 123

Table 5 – References | Tabelle 5 - Refrenzen 125

Table 6a – Definitions in English 127

Tabelle 7b – Definitionen in Deutsch 128

1 Introduction | Einleitung

1.1 Overview | Überblick

Deutsche Telekom Security GmbH (hereinafter referred to as "Telekom Security") provides several Trust Services for issuing certificates to support PKI products offered on the market and customer-specific PKI solutions. On the one hand, Telekom Secruity acts itself as a “(qualified) Trust Service Provider” ((q)TSP) and on the other hand Telekom Security operates the qualified Trust Services of qTSP Deutsche Telekom AG.

As a TSP, Telekom Security operates various certification authorities (CAs) in its Trust Center. These are both Root Certification Authorities (Root CAs) and Subordinate Certification Authorities (Sub CAs) for issuing certificates, both for customers and employees of the Deutsche Telekom AG Group.

In addition, Telekom Security has issued public Sub CA certificates to the "Verein zur Förderung eines Deutschen Forschungsnetzes e. V." (hereinafter referred to as "DFN" for short), which DFN as an independent TSP uses to issue certificates for its affiliated institutions.

Note: There are currently no plans to issue further Sub-CA certificates to DFN or other organizations not affiliated with Deutsche Telekom, so this CP no longer addresses any requirements in this regard. However, the requirements to be met in ongoing operations continue to apply to DFN, so that in the following the term TSP refers to both Telekom Security and DFN, if applicable.

This document is the Certificate Policy (CP) of the Telekom Security Trust Center. It summarizes in the structure of [RFC3647][1] all relevant requirements from the documents referenced in Appendix B that must be implemented by the Trust Services within the scope of this CP.

The scope of this CP comprises all Telekom Security Trust Services via which certificates are issued below the

- public and qualified Root CAs of Telekom Security,
- internal Root CAs of Telekom Security ,

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“)[2] zur Ausgabe von Zertifikaten. Die Telekom Security tritt zum einen selbst als „(qualifizierter) Vertrauensdiensteanbieter“ ((q)VDA) bzw. „(qualified) Trust Service Provider“ ((q)TSP)[2] auf, zum anderen betreibt die Telekom Security die qualifizierten Vertrauensdienste des qVDA Deutsche Telekom AG.

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][1] 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,

[1] In addition, the following chapters have been added to this CP | Zusätzlich wurden folgende Kapitel hinzugefügt
- 3.2.7: Validation of control over a domain | Validierung der Kontrolle über eine Domain
- 3.2.8: Validation of control over an email address | Validierung der Kontrolle über eine E-Mail-Adresse

[2] In Anlehnung an den etablierten Sprachgebrauch werden auch in der deutschen Version die englischen Fachbegriffe verwendet.

- Root CAs issued by the German Federal Office for Information Security (“BSI”) in accordance with [TR3145].

This CP is based on the relevant ETSI standards (see Annex B). The requirements resulting from these ETSI standards apply in principle to all Trust Services subject to this CP, including Trust Services conforming to [TR3145]. Requirements of [TR3145] that supplement or replace the ETSI requirements are marked accordingly.

The following semantics apply to the requirements listed in this document:

- Requirements that are not specifically marked apply in general for all certificate types.
- Requirements highlighted in gray that begin with the specification of one or more certificate types in square brackets apply only to those certificate types.

The following certificate types are distinguished in this document:

- [ETSI] identifies all certificates that are issued by Telekom Security in accordance with ETSI EN 319 411-1 [ETS411-1], ETSI EN 319 411-2 [ETS411-2] or ETSI TS 119 411-6 [ETS411-6].
  Delimitation: These are currently only certificates according to the policies LCP, NCP, DVCP, OVCP and EVCP from [ETS411-1] as well as QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd, QNCP-w and QEVCP-w from [ETS411-2]. No certificates are issued in accordance with IVCP or NCP+, nor are any short-term certificates issued. Requirements in this regard are therefore not addressed in this document.
- [QCP] identifies all EU qualified certificates according to [eIDAS], which are issued in accordance with ETSI EN 319 411-2 [ETS411-2].
- [QCP-n] identifies all EU qualified certificates for natural persons.
- [QCP-l] identifies all EU qualified certificates for legal entities.
- [QCP-n-qscd] identifies all EU qualified certificates for natural persons with use of the private key in a QSCD.
- [QCP-l-qscd] identifies all EU qualified certificates for legal entities with use of the private key in a QSCD.
- [QNCP-w] identifies all EU qualified web server certificates based on [OVCP].
- [QEVCP-w] identifies all EU qualified web server certificates based on [EVCP].
- [TLS] identifies all TLS authentication certificates that are issued in accordance with the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" of the CA/Browser Forum [BR] and the root store policies of Microsoft [MSRP], Mozilla [MOZRP], Google [GCRP] and Apple

- 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.

Für die in diesem Dokument aufgeführten Anforderungen gilt folgende Semantik:

- Anforderungen ohne besondere Markierung gelten grundsätzlich übergreifend für alle Zertifikatstypen.
- Grau hinterlegte Anforderungen, die mit der Angabe eines oder mehrerer Zertifikatstypen in eckigen Klammern beginnen, gelten nur für die betroffenen Zertifikatstypen.

Es werden in diesem Dokument folgende Zertifikatstypen unterschieden:

- [ETSI] kennzeichnet übergreifend alle Zertifikate, die gemäß ETSI EN 319 411-1 [ETS411-1], ETSI EN 319 411-2 [ETS411-2] oder ETSI TS 119 411-6 [ETS411-6] von der Telekom Security ausgestellt werden.
  Abgrenzung: Derzeit sind das ausschließlich Zertifikate gemäß den Policies LCP, NCP, DVCP, OVCP und EVCP aus [ETS411-1] sowie QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd, QNCPw und QEVCP-w aus [ETS411-2]. Es werden keine Zertifikate gemäß IVCP oder NCP+ ausgestellt, ebenso werden keine Kurzzeitzertifikate ausgestellt. Auf diesbezügliche Anforderungen wird daher in diesem Dokument nicht eingegangen.
- [QCP] kennzeichnet übergreifend alle EU qualifizierten Zertifikate nach [eIDAS], die gemäß der ETSI EN 319 411-2 [ETS411-2] ausgestellt werden.
- [QCP-n] kennzeichnet alle EU qualifizierten Zertifikate für natürliche Personen.
- [QCP-l] kennzeichnet alle EU qualifizierten Zertifikate für juristische Personen.
- [QCP-n-qscd] kennzeichnet alle EU qualifizierten Zertifikate für natürliche Personen mit Nutzung des privaten Schlüssels in einer QSCD.
- [QCP-l-qscd] kennzeichnet alle EU qualifizierten Zertifikate für juristische Personen mit Nutzung des privaten Schlüssels in einer QSCD.
- [QNCP-w] kennzeichnet alle auf [OVCP] basierenden EU qualifizierten Web-Server-Zertifikate.
- [QEVCP-w] kennzeichnet alle auf [EVCP] basierenden EU 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.

[APRP] below the public Root CAs of Telekom Security integrated in the root stores.
Delimitation: These are currently only DV, OV and EV certificates. No IV certificates are issued. Requirements in this regard are therefore not ad-dressed in this document.

- [EVCP] identifies all certificates based on [TLS] that also meet the requirements of the "CA/Browser Forum Extended Validation Certificate Guidelines" [EVCG] and the "Extended Validation Certificate Policy" defined in [ETS411-1].
- [SMIME] identifies all S/MIME certificates for email security that are issued in accordance with the "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" of the CA/Browser Forum [SBR] and the root store policies of Microsoft [MSRP], Mozilla [MOZRP], Google Workspace [GWS] and Apple [APRP] below the public Root CAs of Telekom Security integrated in the root stores.
  Delimitation: These are currently only certificates of the Multipurpose generation. No certificates of the Legacy or Strict generations are issued, so this document does not address these requirements.
- [3145] identifies all certificates issued by Telekom Security in accordance with [TR3145] below the BSI root CAs.
- [VS-NfD] identifies all certificates based on [3145] that also meet the requirements for VS-NfD in accordance with the extension [TR3145VS].

The options or obligations to implement the requirements are described by the keywords according to [RFC2119]:

- SHALL indicates an absolute requirement.
- SHALL NOT indicates an absolute prohibition.
- SHOULD indicates a principle requirement, which can only be omitted if there are good reasons.
- SHOULD NOT indicates a principle prohibition, unless there are good reasons for implementation.
- MAY indicates that an item is truly optional.

Trust Services SHALL describe the implementation of the applicable requirements of this CP in their Certification Practice Statements (CPS), also structured according to [RFC3647]. The CPS SHALL address all aspects of this CP and consider all chapters of [RFC3647]. Subchapters that are not applicable SHALL be marked "No stipulation", i.e., these SHALL NOT be left blank or omitted.

Compliance with the requirements of this CP, in its current version, SHALL be explicitly confirmed in the CPS.

[TLS] [SMIME] Where applicable, compliance with the latest versions of the [BR], [SBR], [NCSSR], and [EVCG] SHALL be explicitly confirmed in the CPS and the links to

Abgrenzung: Derzeit sind das ausschließlich DV-, OV- und EV-Zertifikate. Es werden keine IV-Zertifikate ausgestellt. Auf diesbezügliche Anforderungen wird daher in diesem Dokument nicht eingegangen.

- [EVCP] kennzeichnet alle auf [TLS] basierenden Zertifikate, die zusätzlich den Anforderungen der „CA/Browser Forum Extended Validation Certificate Guidelines“ [EVCG] sowie der in [ETS411-1] definierten „Extended Validation Certificate Policy“ genügen.
- [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.
  Abgrenzung: Derzeit sind das ausschließlich Zertifikate der Generation Multipurpose. Es werden keine Zertifikate der Generationen Legacy oder Strict ausgestellt, auf diesbezügliche Anforderungen wird daher in diesem Dokument nicht eingegangen.
- [3145] kennzeichnet alle Zertifikate, die von der Telekom Security gemäß [TR3145] unterhalb der Root-CAs des BSI ausgestellt werden.
- [VS-NfD] kennzeichnet alle auf [3145] basierenden Zertifikate, die zusätzlich 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

the documents of the CA/Browser Forum (http://www.cabforum.org) SHALL be included. In the event of a conflict between this CP or the CPS and the [BR], [SBR] or [EVCG], the regulations from [BR], [SBR] or [EVCG] prevail.

Compliance with the requirements to the current policies of the relevant Root Stores [MSRP], [MOZRP], [GCRP], [GWS] and [APRP] as well as [CCADB] SHALL be explicitly confirmed in the CPS. In the event of a conflict between [MOZRP] and the [BR], the regulations from [MOZRP] shall prevail.

The CPS SHALL be published under a Creative Commons license (CC-BY 4.0, CC-BY-SA 4.0, CC-BY-ND 4.0, CC-0 1.0 or newer versions).

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 jeweils aktuellen Policies der relevanten Root Stores [MSRP], [MOZRP], [GCRP], [GWS] und [APRP] sowie der [CCADB] 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 Document name and identification | Name und Kennzeichnung des Dokuments

This document is named "Certificate Policy of the Telekom Security Trust Center" and is identified by the OID 1.3.6.1.4.1.7879.13.42.

The OID is composed as follows: {iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) T-Telesec (7879) PolicyIdendifier (13) Certificate policy of the Telekom Security Trust Center (42)}

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 participants | PKI-Teilnehmer

1.3.1 Certification Authorities | Zertifizierungsstellen

Telekom Security operates several public as well as internal Root and Sub CAs. It also issues its own Cross Certificates, but not cross certificates to Root or Sub CAs of other TSPs.

Telekom Security does not operate any technically constrained Sub CAs.

The scope of this document also includes the public Sub CAs of the DFN issued by Telekom Security.

The complete hierarchies, i.e., all relevant Root and/or Sub CA certificates in the scope of a CPS, SHALL be listed in the respective CPS.

Note: For the sake of simplicity, the term "CAs" is used below as a synonym for "Root and Sub CAs", i.e., the requirements for "CAs" refer to both Root and Sub CAs,

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.

Telekom Security betreibt keine technisch beschränkten Sub-CAs.

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,

unless otherwise specified. The same applies to the term "CA certificates", which also includes cross certificates.

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 does not operate any technically constrained Sub-CAs.

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

1.3.2 Registration Authorities | Registrierungsstellen

The Registration Authorities (RA) used MAY be both the TSP's internal RAs and external RAs acting on their behalf. The requirements for RAs set out in this document SHALL be implemented equally for internal and external RAs, where applicable.

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.

When using external RAs, the structures, relevant processes as well as their rights and obligations SHALL be described in the respective CPS and appropriate agreements SHALL be met.

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.

For the management of certificates of an organization or devices of this organization or natural persons related to this organization, Enterprise RAs MAY be used as a special form of external RAs.

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.

To setup an Enterprise RA of an organization, the organization SHALL be validated according to Section 3.2.2, the head of the Enterprise RA (contact person of the TSP) as well as the RA staff members responsible for the registration and certificate management activities SHALL be identified according to Section 3.2.3 and their authorization to act as RA staff members and, if necessary, to authorize further RA staff members SHALL be proven according to Section 3.2.5. The TSP SHALL maintain a list of authorized RA staff and provide it to the organization upon request.

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.

If a RA validates certificate applications for its own organization or its employees, an RA employee MAY not validate an application for a certificate in which he himself is the subject.

Wenn eine RA Zertifikatsanträge für die eigene Organisation oder deren Mitarbeiter validiert, DARF ein RA-Mitarbeiter nicht die Validierung eines Antrags zu einem Zertifikat durchführen, in dem er selbst das Subjekt ist.

[TLS] [SMIME] The validation of domain names, IP addresses and the authorization or control of a mailbox SHALL NOT be handed over to external RAs, see Section 4.2.
An Enterprise RA MAY only manage certificates where

- the FQDN set in `subjectAltName`,
- the FQDN portion of the email address set in `subjectAltName` or in the `subjectDN` and
- the name of the organization set in the `subjectDN`

is from the validated namespace of that organization or an affiliate.

[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

- die im `subjectAltName` gesetzten FQDN,
- die FQDN-Anteile der im `subjectAltName` oder im `subjectDN` gesetzten E-Mail-Adressen und
- die im `subjectDN` gesetzten Namen der Organisation

aus dem validierten Namensraum dieser oder einer verbundenen Organisation stammen.

1.3.3 Subscribers | Zertifikatsnehmer

Note: Due to the partially different use of terms in the documents referenced in Annex B, the terms as used in this document are described below.

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.

Subscribers in the context of this CP are natural persons or organizations to whom a certificate is issued and who are legally bound by acceptance of the Terms of Use. A certificate subscriber may also be the subject of a certificate and/or the applicant at the same time.

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.

Organizations in the context of this CP are legal persons or organizational units[3] identified in association with a legal person.
Organizations may be:

- Private Organizations: Non-governmental legal persons whose existence was created by a filing with or an act of the Incorporating Agency or equivalent body
- Government Entities: Government-operated legal persons, agencies, departments, or other related organizational units
- Non-Commercial Entities: International organizations created under a charter, agreement, convention, or equivalent instrument signed by or on behalf of more than one government of a country
- Business Entities: Organizations that are not one of the previously mentioned organizations

Organisationen im Sinne dieser CP sind juristische Personen oder organisatorische Einheiten[5] , die in Verbindung mit einer juristischen Person identifiziert werden. 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.

Subject of a certificate in the context of this CP is the user of the private key named in the certificate in the attributes of the `subjectDN` or the extension `subjectAltName`.

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.

Within the scope of this CP, subjects are

- natural persons,
- natural persons identified in association with an organization,
- organizations,

Subjekte im Geltungsbereich dieser CP können

- natürliche Personen oder
- natürliche Personen, die in Verbindung mit einer Organisation identifiziert werden oder
- Organisationen oder

[3] Organizational units identified in association with a legal entity are hereinafter subsumed under the term “organization”, unless explicitly stated otherwise

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

- devices[4] operated by or on behalf of a natural person or an organization.

The subscribers and subjects in the scope of a CPS SHALL be listed in the respective CPS.

Applicant in the context of this CP is the person who submits the application to the TSP. This is always a natural person who is either
- the subscriber and/or the subject itself,
- an authorized representative of the subscriber (in the case of an organization) or
- another person authorized by the subscriber.

[EVCP] Subscribers MAY only be private organizations or government entities.

Note: "Applicant" as used in this CP is synonymous with "Certificate Requester" as per [EVCG].

In addition to the applicant, the following roles SHALL be implemented:
- **Contract Signer**: A natural person who is explicitly authorized to represent the certificate subscriber and to sign certificate requests on its behalf.
- **Certificate Approver**: A natural person who is explicitly authorized to represent the certificate subscriber and to approve certificate requests on its behalf.

A person MAY be entrusted with more than one of the listed roles and the roles MAY be filled by more than one person.

- Geräte[6], 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 private oder öffentliche Organisationen sein.

Hinweis: Der in dieser CP verwendete Begriff „Antragsteller" ist gleichbedeutend mit „Certificate Requester" gemäß [EVCG].

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.

1.3.4 Relying parties | Zertifikatsnutzer (vertrauende Dritte)

No stipulation.

Keine Vorgabe.

1.3.5 Other participants | Andere Teilnehmer

No stipulation.

Keine Vorgabe.

1.4 Certificate usage | Zertifikatsverwendung

[4] The term "devices" hereinafter also subsumes systems, functions and IT processes, unless explicitly stated otherwise
[6] der Begriff „Geräte" subsummiert nachfolgend auch Systeme, Funktionen und IT-Prozesse, sofern nicht explizit anders aufgeführt

1.4.1 Appropriate certificate uses | Zulässige Verwendung von Zertifikaten

The allowed uses of the certificates SHALL be described in the CPSs, the Terms of Use and, if applicable, the PKI-Disclosure Statements (PDS).

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

1.4.2 Prohibited certificate uses | Unzulässige Verwendung von Zertifikaten

The prohibited uses of the certificates SHALL be described in the CPSs, the terms of use and, if applicable, the PDSs.

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

[EVCP] Certificates SHALL NOT be used for purposes other than TLS server authentication of web servers.

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

1.5 Policy administration | Verwaltung des Dokuments

1.5.1 Organization administering the document | Verwaltende Organisation dieses Dokuments

This document is administered by:
Deutsche Telekom Security GmbH
Trust Center & ID Security
Koblenzer Str. 87-93
57072 Siegen, Germany

Das Dokument wird verwaltet von:
Deutsche Telekom Security GmbH
Trust Center & ID-Security
Koblenzer Str. 87-93
57072 Siegen, Deutschland

1.5.2 Contact person | Ansprechpartner

The contact for this CP is the Trust Center's PKI Compliance Management, which can be reached via email under trustcenter-roots@telekom.de.

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] To report suspected key compromise, misuse, or other types of fraud or inappropriate behavior, well-defined processes SHALL be established. These SHALL be described/published on the TSP's public web pages as well as in the CPSs in Section 1.5.2.

[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] Contacts are the Trust Center's Information Security Officer and his deputy, who can be reached via email under FMB-ISMS-TrustCenter@telekom.de.

[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 Person determining CPS suitability for the policy | Instanz für die Feststellung der Konformität eines CPS zu dieser CP

Responsible for determining the conformity of a CPS to this CP is the Trust Center's PKI Compliance Management, for contact see Section 1.5.2.

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 CPS approval procedures | Genehmigungsverfahren dieser CP und eines CPS

New versions of this CP SHALL be approved by the Trust Center management.

New versions of a CPS based on this CP SHALL first be reviewed by the Trust Center's PKI Compliance Management to determine the conformance to this CP and then be approved by the Trust Center management.

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 Definitions and acronyms | Definitionen und Abkürzungen

Definitions, abbreviations and references are listed in the appendix of this document:

- Appendix A: Abbreviations
- Appendix B: References
- Appendix C: Definitions

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

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

2 Publication and repository responsibilities | Verantwortung für Veröffentlichung und Verzeichnisse

2.1 Repositories | Verzeichnisse

It SHALL be described in the CPSs who maintains which directories containing information about the certificates in the scope of the respective CPS.

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

2.2 Publication of certification information | Veröffentlichung von Informationen zu Zertifikaten

The currently valid version of this document and the relevant superseded versions are published on the web pages of the Telekom Security Trust Center at the following address: https://www.telesec.de/de/service/downloads/pki-repository/

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/

At a minimum, for each Trust Service the following information SHALL be published via suitable online services that can be accessed around the clock:

- Terms of Use in a generally understandable language
- PDS, if available
- CPS
- CA certificates
- status information according to Sections 4.9 and 4.10 for all unexpired certificates issued by them

Zu jedem Trust Service MÜSSEN mindestens

- die Nutzungsbedingungen in einer allgemein verständlichen Sprache,
- sofern vorhanden, das PDS
- 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.

The Terms of Use, PDS, CPSs as well as the CA certificates SHOULD be published in the above-mentioned PKI repository analogously to this CP, unless otherwise specified.

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

The Terms of Use and CPSs SHALL be versioned and provided with validity dates so that they can be easily associated with the certificates issued.

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

In addition, the certificates MAY be published with the subscriber's consent (see Section 4.4.2).

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

[TLS] All issued certificates or alternatively all "pre-certificates" (see Section 4.3.1), including at least all Sub CA certificates (Root CA optional) from its chain, SHALL be published in a sufficient number of "Certificate Transparency Logs" (CTLogs). For the number of CTLogs, see Section 7.1.2 (40).

[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).

For each public Root CA certificate, below which TLS server certificates are issued, test web pages SHALL be provided that are equipped with corresponding TLS server certificates that chain up to the respective Root

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

CA. Web pages with one valid, one expired and one revoked certificate SHALL be provided.

If TLS server certificates according to [EVCG] are also issued below a Root CA, at least the above-mentioned test websites SHALL be provided and be equipped with TLS server certificates according to [EVCG].

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] The CPSs and the audit attestations SHALL (also) be published in English. The translated CPSs SHALL have the same version number as the original CPSs and SHALL NOT differ from them in content.

This CP, the relevant CPS and all necessary information of all CA certificates SHALL be published in the "Common CA Database" (CCADB) in accordance with the CCADB policy (see https://www.ccadb.org) within seven days and kept up to date.

The CPSs SHALL be published on the TSP's official website. The entire history of the CPSs associated with a Root CA and its issued Sub CAs SHALL be kept for the entire time that the Root CA is included as trustworthy in the above-mentioned Root Stores.

[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 von diesen abweichen.

Diese CP, die relevanten CPS sowie alle erforderlichen Informationen zu allen CA-Zertifikaten MÜSSEN in der „Common CA Database“ (CCADB) gemäß der CCADB-Policy (siehe https://www.ccadb.org) innerhalb von sieben Tagen 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] In addition to the CPS a PKI Disclosure Statement (PDS) in the structure according to Annex A of [ETS4111] SHALL be published for each Trust Service at least in English. The https URL to retrieve the PDS SHALL be listed in the `qcStatement qcs-QcPDS`.

In the PDS, it SHALL be pointed out that the TSP with the corresponding Trust Service for the issuance of the qualified certificates must be listed in the EU Trusted List according to [ETS612].

The EU Trust Mark MAY be used by the Qualified Trust Services.

[QCP] Zu jedem Trust Service MUSS darüber hinaus ein „PKI Disclosure Statements“ (PDS) in der Struktur gemäß des Anhang A der [ETS411-1] mindestens in englischer Sprache veröffentlicht werden. Die https-URL zum Abruf des PDS MUSS im `qcStatement qcs-QcPDS` aufgeführt werden.

In den PDS MUSS darauf hingewiesen werden, dass TSP mit dem entsprechenden Trust Service zur Ausgabe der qualifizierten Zertifikate in der EU Trusted List gemäß [ETS612] aufgeführt sein muss.

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

2.3 Time or frequency of publication | Zeitpunkt oder Häufigkeit von Veröffentlichungen

New versions of this CP and the CPSs based on this CP SHALL be published before they become effective.

The time or frequencies of the publications listed in Section 2.2 SHALL be described in the CPSs.

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

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

[TLS] [SMIME] New Root CA certificates SHALL be published at the latest when applying for Root inclusion with one of the Root Stores listed in Section 1.1.

New Sub CA certificates under the Root CAs included in the above-mentioned Root Stores SHALL be published before they are put into operation, but no later than 7 days after their issuance.

[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 attestations SHALL be published no later than 7 days after their issuance.	Audit-Bescheinigungen MÜSSEN spätestens 7 Tage nach ihrer Ausstellung veröffentlicht werden.

2.4 Access controls on repositories

The directories SHALL be publicly available in a read-only manner and SHALL be protected against unauthorized manipulation as well as data loss.	Verzeichnisse MÜSSEN für lesenden Zugriff öffentlich verfügbar sein und MÜSSEN vor unbefugter Manipulation sowie Datenverlust geschützt sein.

3 Identification and Authentication | Identifzierung und Authentifizierung

3.1 Naming | Namensregeln

3.1.1 Types of names | Namensformen

The subject names SHALL be included in all certificates at least in the form of a distinguished name in the attribute of the `subjectDN` in accordance with [X500] , see Section 7.1.4.

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.

Depending on the certificate type, requirements for subject name elements to be included in the `subjectAltName` extension SHALL also be taken into account, see Section 7.1.2.

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.

3.1.2 Need for names to be meaningful | Aussagekraft von Namen

Certificates issued for testing purposes SHALL be clearly identified as such in the `subjectDN`.

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

[ETSI] `commonName` in Sub CA certificates SHALL include a common name of the TSP (not necessarily the full registered name) and be chosen in a language common to the TSP's market.

[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 certificates for natural persons, unless a pseudonym is used, the attributes `surName` and `givenName` SHALL represent the name of the person according to their identity document. For persons with multiple given names, at least one given name SHALL be specified; additional given names MAY be specified in the order desired by the person. Common abbreviations MAY be used. Characters with accents or umlauts MAY be replaced with appropriate ASCII characters. For persons with a single legal name, this SHALL be given in `surName`. The `commonName` SHOULD reflect the name of the person in common form. The same language encoding SHOULD be used for all attributes.

In Zertifikaten für natürliche Personen MÜSSEN, sofern kein Pseudonym verwendet wird, die Attribute `surName` und `givenName` den Namen der Person gemäß dessen Identitätsdokument 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. Der `commonName` SOLLTE den Namen der Person in gebräuchlicher Form wiederspiegeln. Für alle Attribute SOLLTE die gleiche Sprachkodierung verwendet werden.

In certificates issued to natural persons in association with an organization, the certificate attributes `organizationName`, `organizationalUnitName` and `organizationIdentifier`, if set, SHALL reflect the organization.

In Zertifikaten für natürliche Personen in Verbindung mit einer Organisation MÜSSEN die Attribute `organizationName`, `organizationalUnitName` und `organizationIdentifier`, sofern gesetzt, die Organisation widerspiegeln.

In certificates for organizations, `organizationName` SHALL contain the full name of the organization. Common and unambiguous abbreviations MAY be used, or, in

In Zertifikaten für Organisationen MUSS der `organizationName` den vollständigen Namen der Organisation enthalten. Es DÜRFEN gebräuchliche und unmissverständliche Abkürzungen

order not to exceed the maximum length of 64 characters, non-critical name components MAY be omitted if the name is still unambiguously recognizable. The `commonName` SHOULD reflect the name of the organization in a common form.

Endonyms or exonyms MAY be used for geographic indications in `localityName` or `stateOrProvinceName`, but archaic geographic names SHOULD NOT be used.

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. Der `commonName` SOLLTE den Namen der Organisation in gebräuchlicher Form wiederspiegeln.

Für geografische Angaben in `localityName` oder `stateOrProvinceName` DÜRFEN Endonyme oder Exonyme verwendet werden, es SOLLTEN jedoch NICHT veraltete Namen verwendet werden.

3.1.3 Anonymity or pseudonymity of subscribers | Anonymität bzw. Pseudonyme der Zertifikatsnehmer

No stipulation.

Keine Vorgabe.

[TLS] Onion Domain Names SHALL NOT be set.

[TLS] Onion Domain Names DÜRFEN NICHT gesetzt werden.

[SMIME] If a pseudonym is used, a unique identifier of the TSP or, if applicable, an identifier of an Enterprise RA that is unique within the organization, SHALL be set for this purpose.

If a pseudonym is to be set in a certificate, the natural person associated with this pseudonym SHALL be known to the TSP and identified in accordance with Section 3.2.3.

The options for using pseudonyms SHALL be described in the CPS.

[SMIME] 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.

Wenn in einem Zertifikat ein Pseudonym gesetzt werden soll, so MUSS die mit diesem Pseudonym verknüpfte natürliche Person dem TSP bekannt und gemäß Kap. 3.2.3 identifiziert worden sein.

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

3.1.4 Rules for interpreting various name forms | Regeln zur Interpretation verschiedener Namensformen

No stipulation.

Keine Vorgabe.

3.1.5 Uniqueness of names | Eindeutigkeit von Namen

The `subjectDN` of all certificates issued by a CA SHALL be unique and assigned to one subscriber each. However, multiple certificates with the same `subjectDN` MAY be issued for one subscriber.

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.

[TLS] An exception to this is the `subjectDN` in Domain Validated Certificates. Here, a `subjectDN` MAY also be assigned to another subscriber if the subscriber has proven his legal ownership of the domain.

[TLS] 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 Recognition, authentication, and role of trademarks | Erkennung, Authentifizierung und Rolle von Markennamen

No stipulation.

Keine Vorgabe.

[TLS] Trademarks, trade names or DBAs SHALL NOT be included in the `subjectDN` in certificates issued by Telekom Security.

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

3.2 Initial identity validation | Initiale Validierung der Identität

Either direct evidence or attestations from appropriate and authorized sources SHALL be used to initially validate the identity of a natural person or an organization.

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

Evidence MAY be submitted in paper form or electronically.

Nachweise DÜRFEN in Papierform oder elektronisch übermittelt werden.

The evidence provided SHALL be checked for authenticity and integrity to the extent possible.

Die bereitgestellten Nachweise MÜSSEN, soweit möglich, auf Authentizität und Integrität geprüft werden.

Only evidence necessary for verification of identity MAY be requested. Applicants SHOULD be advised to obscure non-required information in submitted supporting documentation (e.g., non-required data fields in copies of identity documents).

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).

The information collected from the subscribers and, if applicable, any deviating applicants, as well as its validation SHALL be described in the CPSs.

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

3.2.1 Method to prove possession of private key | Methoden des Besitznachweises des privaten Schlüssels

No stipulation.

Keine Vorgabe.

[TLS] As part of the application process, an electronic certificate request in PKCS#10 format ("Certificate Signing Request", CSR) SHALL be submitted as proof of possession of the private key, containing at least one domain name or IP address to be included in the certificate.

[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] For key pairs generated by the subscriber, at least the public key and the `subjectDN` attributes SHALL be signed with the private key.

[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 Authentication of organization identity | Authentifizierung der Identität von Organisationen

The methods for authenticating the identity of organizations SHALL be described in the CPS.

To verify an organization's name, address and current status , one of the following methods SHALL be used:

- **QGIS** (Qualified Government Information Source): Verification of data against official registers such as trade or association registers, foundation directories, etc.
- **QIIS** (Qualified Independent Information Source): Verification of data against data files from independent third parties that are considered reliable data sources, e.g. "Dun&Bradstreet", "GLEIF", etc.
- **VPL** (Verified Professional Letter): Verification of data against a written attestation of the correctness of the data by a notary.
  When confirming the correctness of the data via VPL, the VPL SHALL be accompanied by a copy of the relevant supporting documents, if applicable. The authenticity of the VPL SHALL be verified by request through a verified communication method, unless the attestation contains a notarial seal or similar features.
- **TSP-Ident**: Verification of the data by an on-site visit of an authorized representative of the TSP.
- **Official Attestation**: Verification of data by an official attestation. For Government Organizations, the attestation SHALL be done by the organization itself or by an organization superior to it.
- **QSeal**: Verification of a qualified electronic seal of the organization to be identified by means of its qualified seal certificate.
  Note: The seal certificate used for verification SHALL NOT itself have been issued on the basis of a verification of a QSeal of this organization (avoidance of multiple successive identifications by means of QSeal).

In addition, other methods confirmed as equivalent by a conformity assessment body and approved at the national level MAY be used.
Lists of QGISs used by the TSP SHALL be published online in an appropriate and easily accessible manner, including a version history, with sufficient information such as the name, jurisdiction, and website of the QGIS. Publication of this information SHALL be described in the CPS in Section 3.2.

[EVCP] This list SHALL contain the allowed values to the attributes to be included in the certificates listed below:

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

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

Zur Überprüfung des Namens, der Anschrift sowie des aktuellen Status 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 Notar.
  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)`
- `jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3)`

[SMIME] An organization's unique registration number SHALL be validated using QGIS, VPL or GLEIF.

[SMIME] Die eindeutige Registrierungsnummer einer Organisation MUSS mittels QGIS, VPL oder GLEIF validiert werden.

[QCP] An organization's unique registration number SHALL NOT be validated using QIIS.

[QCP] Die eindeutige Registrierungsnummer einer Organisation DARF NICHT mittels QIIS validiert werden.

[NCP] In addition to the methods listed above, to authenticate the identity of an organization, the applicant SHALL be identified according to a method listed in Section 3.2.3. In addition, if the applicant is not a direct representative of the organization, the applicant's authorization SHALL be verified according to Section 3.2.5.

[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 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] QGIS, VPL, or official attestations SHALL be used to authenticate the identity of an organization.
Furthermore, the requirements mentioned above regarding the identification and, if applicable, authorization of the applicant according to Section 3.2.3 apply.

[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 Kap. 3.2.3.

3.2.3 Authentication of individual identity | Authentifizierung der Identität natürlicher Personen

The methods for authenticating the identity of natural persons SHALL be described in the CPS.

One of the following methods SHALL be used to verify the identity of a natural person:

- **TSP-Ident**: Verification of a natural person's identity using a government issued ID by the TSP or an RA.
  Verification MAY be conducted in person or by video and SHALL include the following:
  - verification of the authenticity of the identification document
  - visual comparison of the identification document with the person to be identified
  - If a video procedure is used: verification that the presentation is actually live.

  Automated processes and tools MAY be used, provided compliance with the above requirements is ensured.
- **PostIdent**: Verification of a person's identity by Deutsche Post in accordance with [eIDAS#24].
- **eID**: Verification of a person's identity using online identification in accordance with [eIDAS#24].
- **VPL:** (Verified Professional Letter): Verification of data against a written attestation of the correctness of the data by a notary.
  The attestation SHALL include a copy of relevant documentation, if applicable. The authenticity of the attestation SHALL be verified by means of request through a verified communication method, unless the attestation contains a notarial seal or comparable features.
- **QES**: Verification of the identity of a person by means of verification of a qualified electronic signature generated by that person as part of the application or identification process. Required identity attributes

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 Notar.
  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.

that are not apparent from the signature certificate being verified SHALL be obtained and verified by other appropriate means.
Note: The signature certificate used for verification SHALL NOT itself have been issued on the basis of a verification of a QES of this person (avoidance of multiple successive identifications by means of QES).

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).

In addition, other methods confirmed as equivalent by a conformity assessment body and approved at the national level MAY be used.

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

If methods based on evidence with a limited validity are used to verify identity, it SHALL be ensured that the evidence is still valid at the time of verification.

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.

[SMIME] **Enterprise-RA**: For purposes of verifying the identity of an individual associated with an organization, data maintained by the organization MAY alternatively be used to prove the identification of that individual by that organization's Enterprise RA.

[SMIME] **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.

[QCP] Enterprise-RA as well as Video identification procedures SHALL NOT be used.

[QCP] Enterprise-RA und Videoidentverfahren DÜRFEN NICHT verwendet werden.

3.2.4 Non-verified subscriber information | Nicht überprüfte Informationen

The CPS SHALL specify information used but not verified, if applicable.

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

3.2.5 Validation of authority | Validierung der Bevollmächtigung

As proof of authorization to apply for and manage certificates on behalf of an organization, a legally signed or sealed power of attorney from the organization to be represented SHALL be submitted, unless the applicant is directly authorized to represent the organization.

Als Nachweis der Berechtigung, Zertifikate im Namen einer Organisation beantragen und managen zu dürfen, MUSS eine rechtsgültig unterschriebene oder gesiegelte Vollmacht der zu vertretenden Organisation vorgelegt werden, sofern der Antragsteller nicht direkt vertretungsberechtigt ist.

As proof of authorization to apply for and manage certificates on behalf of another natural person, a legally valid signed power of attorney from the person being represented SHALL be submitted.

Als Nachweis der Berechtigung, Zertifikate im Namen einer anderen natrülichen Person beantragen und managen zu dürfen, MUSS eine rechtsgültig unterschriebene Vollmacht der zu vertretenden Person vorgelegt werden.

[EVCP] Alternatively, to validate an authorization to sign or approve certificate requests, confirmation MAY be obtained from an authorized representative of the organization via a verified communication method.

[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 Criteria for interoperation | Kriterien für Interoperabilität

No stipulation.

Keine Vorgabe.

3.2.7 Validation of control over a domain or IP-address | Validierung der Kontrolle über eine Domain oder IP-Adresse

No stipulation.

Keine Vorgabe.

[TLS] Each fully qualified domain name (FQDN) SHALL be validated using one of the following methods which are described in more detail in [BR#3.2.2.4]:

- Constructed email to the domain contact as per [BR#3.2.2.4.4],
- DNS change as per [BR#3.2.2.4.7],
- Validation of the applicant as a domain contact as per [BR#3.2.2.4.12],
- Email to the DNS CAA email contact as per [BR#3.2.2.4.13],
- Email to the DNS CAA TXT record email contact as per [BR#3.2.2.4.14],
- Telephone call to the DNS TXT Record contact as per [BR#3.2.2.4.16],
- Telephone call to DNS CAA contact as per [BR#3.2.2.4.17],
- Agreed change of web page v2 as per [BR#3.2.2.4.18] ,
- Agreed change of web page ACME as per [BR#3.2.2.4.19],
- TLS using ALPN as per [BR#3.2.2.4.20],
- DNS Labeled with Account ID - ACME as per [BR#3.2.2.4.21],
- DNS TXT Record with Persistent Value as per [BR#3.2.2.4.22].

At least one of the methods as per [BR#3.2.2.4.7], [BR#3.2.2.4.18], [BR#3.2.2.4.19] oder [BR#3.2.2.4.20] SHALL be supported.

Beginning March 15, 2026, all DNS queries related to validating control over a domain SHALL undergo DNSSEC validation against the IANA DNSSEC Root Trust Anchor from the primary network perspective, as specified in [BR#3.2.2.4].

After a successful validation of an FQDN according to one of the methods from [BR#3.2.2.4] listed above, the validation of further FQDNs or Wildcard Domain Names ending with the domain labels of the validated FQDN MAY be omitted. This does not apply to validations according to [BR#3.2.2.4.8], [BR#3.2.2.4.18], [BR#3.2.2.4.19] and [BR#3.2.2.4.20].

[TLS] Jeder vollqualifizierte Domain-Name (FQDN) MUSS mithilfe einer der folgenden Methoden validiert werden, die in [BR#3.2.2.4] ausführlicher beschrieben sind:

- konstruierte E-Mail an den Domain-Kontakt gemäß [BR#3.2.2.4.4],
- DNS-Veränderung gemäß [BR#3.2.2.4.7],
- 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 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],
- DNS mit ACME Account-ID gemäß [BR#3.2.2.4.21],
- DNS-TXT-Record mit persistenten Werten gemäß [BR#3.2.2.4.22].

Es MUSS mindestens eine der Methoden gemäß [BR#3.2.2.4.7], [BR#3.2.2.4.18], [BR#3.2.2.4.19] oder [BR#3.2.2.4.20] unterstützt werden.

Ab 15.03.2026 MUSS für alle DNS-Abfragen im Zusammenhang mit der Validierung der Kontrolle über eine Domain eine DNSSEC-Validierung zum IANA DNSSEC Root Trust Anchor aus der primären Netzwerkperspektive gemäß [BR#3.2.2.4] durchgeführt werden.

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].

For each Wildcard Domain Name to be included in a certificate, it SHALL be verified that the FQDN part is of type "registry-controlled" or "public suffix". A regularly updated "public-suffix-list" (PSL) MAY be used for this check. If such a PSL is used for checking, only the "ICANN domains" SHOULD be accepted.

Validation of control over an IP address SHALL be performed according to one of the following methods:

- Agreed upon change to the web site in accordance with [BR#3.2.2.5.1]
- Email, fax, SMS, or mail to the IP address contact in accordance with [BR#3.2.2.5.2]
- Reverse address lookup in accordance with [BR#3.2.2.5.3]
- Phone call to IOP address contact in accordance with [BR#3.2.2.5.5]
- ACME "http-01" method for IP addresses in accordance with [BR#3.2.2.5.6]
- ACME "tls-alpn-01" method for IP addresses in accordance with [BR#3.2.2.5.7]

With the exception of the methods as per [BR#3.2.2.4.4], [BR#3.2.2.4.12], [BR#3.2.2.5,2] and [BR#3.2.2.5.5], validation SHALL be performed via different network perspectives as per [BR#3.2.2.9].

The methods used according to [BR#3.2.2.4] or [BR#3.2.2.5] SHALL be listed in the CPSs including a reference to the relevant Section of the [BR].

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].

Mit Ausnahme der Methoden gemäß [BR#3.2.2.4.4], [BR#3.2.2.4.12], [BR#3.2.2.5,2] und [BR#3.2.2.5.5] MUSS die Validierung über verschiedene Netzwerkperspektiven gemäß [BR#3.2.2.9] erfolgen.

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 Validation of control over an email address | Validierung der Kontrolle über eine E-Mail-Adresse

No stipulation.

Keine Vorgabe.

[SMIME] To verify the applicant's control over the email addresses referenced in the certificate, or the applicant's authorization to act on behalf of the actual owner of the email addresses, one of the following methods SHALL be used:

a) Validation of the applicant's control over the domain portion of the email address as per [SBR#3.2.2.1] (e.g. in the case of an Enterprise RA).
b) Validation of control over each individual mailbox via validation email as per [SBR#3.2.2.2] or
c) Validation of the applicant as the operator of the mail server to which the e-mails of the e-mail address to be validated are sent as per [SBR#3.2.2.3] (e.g. in the case of an Enterprise RA).
d) Validating control over mailbox using ACME extensions as per [SBR#3.2.2.4]

To validate domain names, the methods listed in Section 3.2.7 SHALL be used.

[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 eine der folgenden Methoden angewendet werden:

a) Validierung der Kontrolle des Antragstellers über den Domänen-Anteil der E-Mail-Adresse gemäß [SBR#3.2.2.1] (z.B.im Fall einer Enterprise-RA),
b) Validierung der Kontrolle über jede einzelne Mailbox per Validierungs-E-Mail gemäß [SBR#3.2.2.2] oder
c) Validierung des Antragstellers als Betreiber des Mailservers, an den die E-Mails der zu validierenden E-Mail-Adresse gesendet werden gemäß [SBR#3.2.2.3] (z.B.im Fall einer Enterprise-RA) oder
d) Validierung der Kontrolle über jede einzelne Mailbox mithilfe von ACME-Erweiterungen gemäß [SBR#3.2.2.4].

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

The validation of the control over a mailbox by means of a validation email SHALL be performed using individual and temporary valid random values according to [SBR#3.2.2.2].	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.
The verification methods used SHALL be described in the CPSs.	Die angewandten Verifizierungsmethoden MÜSSEN in den CPS beschrieben werden.

3.3 Identification and authentication for re-key requests | Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung

3.3.1 Identification and authentication for routine re-key | Identifizierung und Authentifizierung für routinemäßige Schlüsselerneuerung

The requirements according to Section 3.2 apply.	Es gelten die Anforderungen gemäß Kap. 3.2.
Existing evidence MAY be reused for the validation of identity, taking into account the applicable legal situation and the remaining validity of the evidence (see Section 4.2.1).	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 Identification and authentication for re-key after revocation | Identifizierung und Authentifizierung für Schlüsselerneuerung nach einer Sperrung

Revoked certificates SHALL NOT be renewed. After a revocation, a new certificate SHALL be requested.	Gesperrte Zertifikate DÜRFEN NICHT erneuert werden. Nach einer Sperrung MUSS ein neues Zertifikat beantragt werden.
Existing evidence MAY be reused for the validation of identity, taking into account the applicable legal situation and the remaining validity of the evidence (see Section 4.2.1).	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.

3.4 Identification and authentication for revocation request | Identifizierung und Authentifizierung von Sperranträgen

The methods for identification and authentication of revocation requests SHALL be described in the CPSs.	Die Methoden zur Identifizierung und Authentifizierung von Sperranträgen MÜSSEN in den CPS festgelegt werden.

4 Certificate Life-cycle operational requirements | Betriebliche Anforderungen an den Zertifikats-Lebenszyklus

The requirements of this Section SHALL be implemented for all certificates, including certificates issued by the TSPs for themselves or their employees.

Unless explicitly stated otherwise, the requirements apply to the certificates of all hierarchy levels.

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 Certificate Application | Zertifikatsantrag

4.1.1 Who can submit a certificate application? | Zertifikatsantragsberechtigte

The persons entitled to apply for certificates as well as their possible roles SHALL be described in the CPSs.

To avoid conflicts of interest, the TSPs SHALL NOT be the applicants for subscriber certificates. This excludes organizations that perform registration activities and issue certificates for themselves or persons associated with them. Exceptions SHALL be described in the CPSs.

[EVCP] Organizations for which a certificate is requested SHALL be based in Germany, Austria or Switzerland.

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.

[EVCP] Organisationen, für die ein Zertifikat beantragt wird, MÜSSEN ihren Sitz in Deutschland, Österreich oder der Schweiz haben.

4.1.2 Enrollment process and responsibilities | Antragsprozess und -verantwortlichkeiten

The application processes including the interfaces to be used SHALL be described in the CPSs.

Certificate applications SHALL be provided by the applicants with the following information:

- at least one contact information (physical address, e-mail address, or other information),
- all attributes to be included in the `subjectDN` or `subjectAltName`,
- the confirmation of knowledge and acceptance of the Terms of Use,
- consent to the recording of data collected as part of the certificate management process,
- if applicable, a statement regarding the publication of the certificate.

A certificate application MAY be used to apply for multiple certificates. However, it SHALL be ensured that the acceptance of the Terms of Use for each certificate is given.

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.

This data SHALL either be provided by the applicant at the time of application or confirmed by the applicant after querying reliable sources.

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

Certificate applications MAY be submitted in electronic form. In this case, however, the applications, including acceptance of the Terms of Use, SHALL be confirmed by a traceable action (e.g. checking a box in the web application form) or signed electronically.

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] Missing information SHALL be provided or confirmed by the Certificate Approver or Contract Signer. This does not apply to the value to be set in `businessCategory`, which MAY also be set by the TSP without consulting the applicant.

[EVCP] Fehlende Informationen MÜSSEN vom Antragsgenehmiger oder Antragsunterzeichner bereitgestellt oder bestätigt werden. Davon ausgenommen ist der in `businesscategory` zu setzende Wert, der auch vom TSP ohne Rückfrage beim Antragsteller gesetzt werden DARF.

[QCP] Electronically submitted certificate applications SHOULD be provided with at least an advanced electronic signature or an advanced electronic seal.

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

[VS-NfD] The application process SHALL be released by the security officer.

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

4.2 Certificate application processing | Bearbeitung der Zertifikatsanträge

Certificate applications SHALL be checked for correctness, completeness and authorization.

Zertifikatsanträge MÜSSEN auf Korrektheit, Vollständigkeit und Autorisierung geprüft werden.

The manual processing steps listed below SHALL be performed by trusted personnel (see also Section 5.2.1).

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

The processing of applications or parts thereof MAY be outsourced to external RAs. In this case, it SHALL be ensured that the process as a whole meets the requirements of this CP. Accordingly, the external RAs SHALL be identified and authenticated and it SHALL be ensured that information is securely exchanged between the external RAs and the TSP.

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] This excludes validation over control of a domain or IP address according to Section 3.2.7, which SHALL be performed by the TSP itself.

[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] This excludes the validation of the Authorization Domain Name (according to [BR]) of the domain part of the email address, which SHALL be performed by the TSP itself.

[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 Performing identification and authentication functions | Durchführung der Identifizierung und Authentifizierung

The subjects of the certificates and, if different, the applicants SHALL be identified according to the methods described in Section 3.2.

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.

The authorization of an applicant SHALL be checked in accordance with Section 3.2.5 if the applicant is not also the subject or, in the case of an organization, an authorized representative of the organization.

Die Bevollmächtigung eines Antragstellers MUSS gemäß Kap. 3.2.5 geprüft werden, wenn der Antragsteller nicht zugleich auch der Zertifikatsnehmer bzw. -im Falle einer Organisation- ein Vertretungsberechtiger der Organisation ist.

[TLS] For organization-validated certificates, verification of authorization in accordance with section 3.2.5 is not necessary if the applicant has been verified as an employee of the applicant organization using a reliable method of communication.

[TLS] Bei Organisations-validierten Zertifikaten ist die Prüfung der Bevollmächtigung gemäß Kap. 3.2.5 nicht erforderlich, sofern der Antragsteller über eine zuverlässige Methode der Kommunikation als Mitarbeiter der antragstellenden Organisation verifziert wurde.

If the subject of a certificate is a natural person, then the following SHALL be validated:
- Full name of the person
- Date and place of birth or reference to an official identity document or other attributes that can be used for unique identification

Ist das Subjekt eines Zertifikats eine natürliche Person, so MÜSSEN überprüft werden:
- 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

If the subject of a certificate is a natural person identified in association with an organization, then the following SHALL additionally be verified:
- Full name and legal status of the organization
- Relevant registration information of the organization
- Affiliation of the natural person with the organization
- Confirmation by the organization and the natural person that the attributes reflect the organization

Ist das Subjekt eines Zertifikats eine natürliche Person in Verbindung mit einer Organisation, so MÜSSEN zusätzlich überprüft werden:
- Der vollständige Name und Rechtsstand der Organisation
- Alle relevanten Registrierungsinformationen der Organisation
- Die Zugehörigkeit der natürlichen Person zur Organisation
- Bestätigung der Person und der Organisation, dass die Attribute die Organisation korrekt widerspiegeln

If the subject of a certificate is an organization, the following SHALL be verified:
- Full name of the organization
- Any relevant registration information of the organization
- A nationally recognized identity number or other attributes that can be used to distinguish the organization as much as possible from others with the same name
- If applicable, the organization's affiliation with the organizational unit identified in association with that organization

Ist das Subjekt eines Zertifikats eine Organisation, so MÜSSEN überprüft werden:
- Der vollständige Name der 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

If the subject of a certificate is a device, the identifier of the device (e.g. Internet domain name or mailbox address) SHALL be checked.

Ist das Subjekt eines Zertifikats ein Gerät MUSS die Kennung des Geräts (z. B. Internet Domain Name oder Mailbox-Adresse) überprüft werden.

If the subject of a subscriber certificate is a device or system operated by a natural person or an organization, then both the identifier of the device or system (e.g., Internet domain name) and the data of the natural person or organization SHALL additionally be verified.

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

All information to be included in a certificate SHALL be verified.

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

[3145] When validating an identity, it SHALL be checked whether the subscriber has already been registered before. In this case, all further certificates SHALL be assigned to the registered subscriber, so that in case of suspension of the subscriber, all certificates of this subscriber can be suspended or revoked simultaneously according to the Terms of Use.

[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] A validation performed MAY be used to issue further certificates within the following time periods:

- Validations of data according to Section 3.2, without Section 3.2.7 and 3.2.8:
  - [SMIME] 825 days
  - [TLS] 398 days
- Validations according to Section 3.2.7 resp. 3.2.8 a): 200 days
- Validations according to Section 3.2.8 b): 30 days
- Validations according to Section 3.2.8 c): 398 days

[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:
  - [SMIME] 825 Tage
  - [TLS] 398 Tage
- Validierungen gemäß Kap. 3.2.7 bzw. 3.2.8 a): 200 Tage
- Validierungen gemäß Kap. 3.2.8 b): 30 Tage
- Validierungen gemäß Kap. 3.2.8 c): 398 Tage

[TLS] To verify the authenticity of an application for an Organization Validated Certificate, confirmation SHALL be obtained via a reliable method of communication with an entity of the organization that is considered reliable.

Organizations SHALL be offered the opportunity to nominate authorized persons to apply for certificates. If an organization has designated eligible individuals in writing, applications SHALL NOT be accepted from individuals other than the designated individuals. Upon written request from an organization, a list of the organization's designated eligible individuals SHALL be provided.

[TLS] Die Prüfung der Authentizität eines Antrags für ein Organisations-validiertes Zertifikat MUSS über eine zuverlässige 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] As part of the authentication of the organization's identity according to Section 3.2.2, the type of organization SHALL also be defined and its legal, physical and operational existence SHALL be verified. The verification of the legal existence also includes, if applicable, the verification or acquisition of registration numbers or dates of incorporation, representative authorities or persons in charge and, if applicable, relationships between organizations and parent or subsidiary companies or shareholdings. The verification of physical and operational existence also includes the verification of the organization's address and a reliable means of communication with the organization.

Furthermore, it SHALL be verified that the application is signed by an authorized Contract Signer and an authorized Certificate Approver.
For this purpose,

- their authorization according to Section 3.2.5 SHALL be verified, if they are not directly authorized to represent the organization,

[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 sowie einer verlässlichen Kommunikationsmöglichkeit mit 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

- it SHALL be verified via a verified method of communication, that the signatures were actually executed by these designated persons in the assigned roles.

As an alternative to the handwritten signature of the application by the Contract Signer and the Certificate Approver, the following methods MAY also be accepted:
- advanced or qualified electronic signatures of the persons mentioned above
- confirmation by the persons mentioned above via a web front-end, provided that they have been appropriately registered before and authenticate themselves via a secure procedure on the web front-end.

In these cases, the additional confirmation of the signature provided by means of verified communication MAY be waived.
After successful completion of all validations, a thorough cross-check of all validations performed SHALL be performed by another RA employee who was not involved in the validations themselves.

Validations performed MAY only be reused for the issuance of further certificates within 398 days of obtaining the evidence.

[VS-NfD] The subscriber's security clearance SHALL be verified with respect to the use of the PKI.

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 nach Einholen der Nachweise wiederverwendet werden.

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

4.2.2 Approval or rejection of certificate applications | Genehmigung oder Ablehnung von Zertifikatsanträgen

Applications MAY only be approved after successful identification and authentication in accordance with Section 4.2.1.

If a key generated by the subscriber is submitted for an application, the possession or control of the private key SHALL be checked. In the case of a key being submitted in the form of a PKCS#10 request, its signature SHALL be checked. In addition, it SHALL be checked whether the presented key meets the requirements of Sections 6.1.5 and 6.1.6. In case of a negative verification result, the application SHALL be rejected.

[TLS] [SMIME] If a key is submitted in an application whose corresponding private key
- was demonstrably generated by means of a faulty method or
- can be easily calculated with a proven or established method, e.g. if it is a "Debian weak key" or
- is known to be compromised (see also Section 4.9.1),

the application SHALL be rejected.

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] [SMIME] Within 8 hours or the time specified in the TTL of the CAA records before issuing a certificate, it SHALL be checked in accordance with [BR#3.2.2.8] and [BR#3. 2.2.9] resp. [SBR#4.2.2.1] and [SBR#4.2.2.2] via different network perspectives for all `dNSNames` (TLS) to be included in the certificate resp. the domain portions of the `rfc822Names` (S/MIME) in the `subjectAltName` using the respective CAA records to check whether Telekom Security is authorized to issue the certificate, i.e., either “telesec.de” SHALL be listed in the property tags listed below or they SHALL be empty:

- [TLS] For requests for certificates with one or more FQDN: `issue`
- [TLS] For requests for certificates with wildcards: `issuewild`
- [SMIME] `issuemail`

From March 15, 2026, DNSSEC validation against the IANA DNSSEC Root Trust Anchor SHALL be performed for all DNS queries related to CAA checking from the primary network perspective in accordance with [BR#3.2.2.8.1] and [SBR#4.2.2.1.1].

[TLS] [SMIME] Innerhalb von 8 Stunden bzw. der in der TTL der CAA-Records angegebenen Zeit vor der Ausstellung eines Zertifikats MUSS gemäß [BR#3.2.2.8] und [BR#3.2.2.9] bzw. [SBR#4.2.2.1] und [SBR#4.2.2.2] über verschiedene Netzwerkperspektiven für alle in das Zertifikat aufzunehemenden `dNSNames` (TLS) bzw. die Domain-Anteile der `rfc822Names` (S/MIME) mittels der jeweiligen CAA-Records geprüft werden, ob Telekom Security berechtigt ist, das Zertifikat auszustellen, d.h. in den nachfolgend aufgeführten property tags MUSS entweder "telesec.de" aufgeführt sein oder diese MÜSSEN leer sein:

- [TLS] Bei Anträgen zu Zertifikaten mit einem oder mehreren FQDN: `issue`
- [TLS] Bei Anträgen zu Zertifikaten mit Wildcards: `issuewild`
- [SMIME] `issuemail`

Ab 15.03.2026 MUSS für alle DNS-Abfragen im Zusammenhang mit der CAA-Prüfung eine DNSSEC-Validierung zum IANA DNSSEC Root Trust Anchor aus der primären Netzwerkperspektive gemäß [BR#3.2.2.8.1] bzw. [SBR#4.2.2.1.1] durchgeführt werden.

[TLS] Where applicable, additional required validations for "high risk certificate requests" SHALL be implemented.

In addition, it SHALL be verified that both the applicant organization and the acting persons are not included in the denied lists to be considered.

[TLS] 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] Certificate applications that are to contain wildcards or IP addresses SHALL be rejected.

[EVCP] Anträge zu Zertifikaten, die Wildcards oder IP-Adressen enthalten sollen, MÜSSEN abgelehnt werden.

[QCP-l-qscd] [QCP-n-qscd] If a key is submitted that is not guaranteed to be from a key pair generated in a QSCD, the application SHALL be rejected.

[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] Certificate requests from suspended subscribers SHALL be rejected.

[3145] Zertifikatsanträge von suspendierten Endteilnehmern MÜSSEN abgelehnt werden.

4.2.3 Time to process certificate applications | Fristen für die Bearbeitung von Zertifikatsanträgen

No stipulation.

Keine Vorgabe.

4.3 Certificate issuance | Zertifikatsausstellung

4.3.1 CA actions during certificate issuance | TSP-Aktivitäten während der Zertifikatsaustellung

The integrity and authenticity SHALL be ensured with appropriate (technical, organizational or personnel).

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

The process of issuing the certificates SHALL be securely linked to the associated registration and, to the public key provided by the applicant resp. the keys generated by the TSP.

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 CA certificate issuance | Ausstellung von CA-Zertifikaten

CA certificates SHALL be issued in the secure environment of the Trust Center during a ceremony. The roles involved as well as their tasks and responsibilities before, during and after the ceremony SHALL be defined and documented.

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.

The individual steps of the ceremony SHALL follow a defined protocol and SHALL be documented in it.

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

The issuance SHALL be performed by at least two trusted employees of the Trust Center, and the following requirements apply:

- Each of the two employees SHALL have knowledge of only a portion of the activation data required for certificate issuance.
- The two employees SHALL act in different roles.

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.

For each new CA certificate, new keys SHALL be used.

Für jedes neue CA-Zertifikat MÜSSEN neue Schlüssel verwendet werden.

When issuing Sub CA certificates, the hash value of the public key or the CSR containing the public key SHALL be verified to prove the authenticity and integrity of the key.

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.

An internal auditor (see Section 8.2) SHALL monitor the ceremony and confirm its correct execution in the protocol.

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

[TLS] [SMIME] Both an internal and a qualified external auditor (see Section 8.2) SHALL monitor the ceremony and confirm its correct execution in the protocol.

[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 Subscriber certificate issuance | Ausstellung von Endteilnehmer-Zertifikaten

In the case where the keys for the subscribers are generated by a TSP, the confidentiality of the keys SHALL be ensured in the generation process.

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

[TLS] Subscriber certificates
- SHALL be verified by appropriate lint tools and
- SHALL be published as "pre-certificates" in a sufficiently large number of CTLog servers (Certificate Transparency according to [RFC6962])

before issuance.

The time-stamped confirmations returned from the CTLog servers SHALL be included in the “leaf certificates” as „Embedded Signed Certificate Timestamps“ (SCT). Regarding the number of CTLogs see Section 7.1.2.

[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.

[SMIME] Subscriber certificates SHALL be verified by appropriate lint tools.

[SMIME] Endteilnehmer-Zertifikate MÜSSEN vor Ausstellung durch geeignete Lint-Tools geprüft werden.

[3145] If the use of cryptographic tokens is required
- it SHALL be ensured by technical measures that the supplied public key is correctly assigned to the token and the registration data,
- it SHALL be ensured that the correct public key of the selected token is included in the certificate and that the certificate is stored on the correct token,
- it SHALL be ensured that the personalized token is sent to the correct recipient,
- the handover of the token SHALL be designed in such a way that a token intercepted by an attacker cannot be used, e.g. by an activation required to use the token, which can only be performed by the authorized recipient using activation data passed to him via a separate channel.

[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 in das 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] The specifications from [VSA] SHALL be considered for the protection of the keys according to their classification.

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

4.3.2 Notification to subscriber by the CA of issuance of certificate | Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines Zertifikats

Subscribers SHALL be informed about the issuance of the certificates.

If applicable, the certificates SHALL be handed over to the subscribers in a usable form, eventually at a later date.

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 Certificate acceptance | Zertifikatsannahme

4.4.1 Conduct constituting certificate acceptance | Verhalten, das die Annahme eines Zertifikats bestätigt

No stipulation.

Keine Vorgabe.

4.4.2 Publication of the certificate by the CA

Certificates MAY be published with the consent of the subscriber but they SHALL NOT be published without consent.

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

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

Keine Vorgabe.

[TLS] CA certificates SHALL be published in the CCADB, subscriber certificates resp. the corresponding pre-certificates in multiple CTLog servers (see Section 4.3.1).

[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 Key pair and certificate usage | Schlüssel- und Zertifikatsnutzung

4.5.1 Private key and certificate usage | Nutzung des privaten Schlüssels und des Zertifikats

The purposes of use of the private keys and certificates SHALL be described in the CPSs.

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

4.5.2 Relying party public key and certificate usage | Nutzung des öffentlichen Schlüssels und des Zertifikats durch Dritte

Relying parties SHOULD comply with the requirements for the use and verification of certificates and public keys set out in the Terms of Use.

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

4.6 Certificate renewal | Zertifikatserneuerung unter Beibehaltung der Schlüssel

4.6.1 Circumstance for certificate renewal | Umstände für ein Renewal

The circumstances under which a renewal is allowed SHALL be defined in the CPSs. Among others, the aspects of key weakening as well as the requirement for sufficient

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

key lengths and permissible algorithms until the end of the validity of the new certificate, SHALL be considered.

bis zum Gültigkeitsende des neuen Zertifikats ausreichenden Schlüssellängen und zulässige Algorithmen betrachtet werden.

Certificates SHALL NOT be renewed if they have been revoked.

Zertifikate DÜRFEN NICHT erneuert werden, wenn diese gesperrt wurden.

Certificates SHALL NOT be renewed if any information in the certificates has changed.

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

4.6.2 Who may request renewal | Antragsberechtigte für ein Renewal

No stipulation.

Keine Vorgabe.

4.6.3 Processing certificate renewal requests | Verarbeitung von Anträgen auf Renewal

If the current Terms of Use have been changed from the Terms of Use in effect at the time the preceding certificate was applied for, acceptance of these new Terms of Use SHALL be obtained from the subscriber prior to issuance of a new certificate.

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.

Prior to renewal, the validity of the preceding certificate and the original submitted identification data and attributes of the subject SHALL be verified. Applications SHALL be complete, accurate, up-to-date, and authorized.

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 Notification of new certificate issuance to subscriber | Benachrichtigung des Zertifikatsnehmers über die Ausstellung neuer Zertifikate

See Section 4.3.2.

Siehe Kap. 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate | Verhalten, das die Annahme eines erneuerten Zertifikats bestätigt

See Section 4.4.1.

Siehe Kap. 4.4.1.

4.6.6 Publication of the renewal certificate by the CA | Veröffentlichung erneuerter Zertifikate durch die TSP

See Section 4.4.2.

Siehe Kap. 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities | Information Dritter über die Ausstellung neuer Zertifikate durch die TSP

See Section 4.4.3.

Siehe Kap. 4.4.3.

4.7 Certificate re-key | Zertifikatserneuerung mit neuen Schlüsseln

4.7.1 Circumstance for certificate re-key | Umstände für eine Schlüsselerneuerung

The circumstances under which re-keying is permitted SHALL be described in the CPSs.

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

Re-keying SHALL NOT be allowed for certificates that have been revoked.

Zertifikate DÜRFEN NICHT erneuert werden, wenn diese gesperrt wurden.

Re-keying SHALL NOT be allowed if any information in the certificates has changed.

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

4.7.2 Who may request certification of a new public key | Antragsberechtigte für eine Schlüsselerneuerung

No stipulation.

Keine Vorgabe.

4.7.3 Processing certificate re-keying requests | Verarbeitung von Anträgen auf Schlüsselerneuerung

If the current Terms of Use have been changed from the Terms of Use in effect at the time the preceding certificate was applied for, the new Terms of Use SHALL be accepted by the subscriber before issuing a new certificate.

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.

Prior to re-keying the validity of the expiring certificate and the original submitted identification data and attributes SHALL be verified. Applications SHALL be complete, accurate, up-to-date, and authorized.

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 the new certificate, the same expiration date SHALL be set as in the preceding certificate.

[EVCP] In einem erneuerten Endteilnehmer-Zertifikat MUSS das gleiche Ablaufdatum wie im ursprünglichen Zertifikat gesetzt werden.

4.7.4 Notification of new certificate issuance to subscriber | Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines erneuerten Zertifikats

See Section 4.3.2.

Siehe Kap. 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate | Verhalten, das die Annahme eines erneuerten Zertifikats bestätigt

See Section 4.4.1.

Siehe Kap. 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA | Veröffentlichung erneuerter Zertifikate durch die TSP

See Section 4.4.2.

Siehe Kap. 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities | Information Dritter über die Ausstellung neuer Zertifikate durch den TSP

See Section 4.4.3.

Siehe Kap. 4.4.3.

4.8 Certificate modification | Änderung von Zertifikatsdaten

4.8.1 Circumstance for certificate modification | Umstände für eine Änderung von Zertifikatsdaten

The circumstances under which a modification of certificate data is allowed or required SHALL be described in the CPSs.

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

If the original key is to be reused when modifying certificate data, the aspects of key weakening and the requirement for sufficient key lengths and permissible algorithms until the new certificate expires, SHALL be considered.

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.

If there is suspicion or evidence of compromise of the key or the preceding certificate has been revoked due to a security incident, the key SHALL NOT be reused.

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.

Subscribers SHALL be required to notify the TSP of the change of registered data in the validity period of the certificates issued based on the registered data. Subscribers SHALL be informed about the processes in case of change of certificate data.

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 Who may request certificate modification

See Section 4.1.1.

Siehe Kap. 4.1.1.

4.8.3 Processing certificate modification requests

If the current Terms of Use have been changed from the Terms of Use in effect at the time the preceding certificate was applied for, the acceptance of these new Terms of Use SHALL be obtained from the subscriber before issuing a new certificate.

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.

Before modifying certificate data, the validity of the expiring certificate and any unmodified subject identification data and attributes originally submitted SHALL be verified. Modified information SHALL be validated and registered according to Section 3.2. The data SHALL be complete, accurate, up-to-date, and authorized.

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] The generation of new keys SHALL be enforced.

[3145] Die Generierung neuer Schlüssel MUSS erzwungen werden.

4.8.4 Notification of new certificate issuance to subscriber

See Section 4.3.2.

Siehe Kap. 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

See Section 4.4.1.

Siehe Kap. 4.4.1.

4.8.6 Publication of the modified certificate by the CA

See Section 4.4.2.

Siehe Kap. 4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

See Section 4.4.3.

Siehe Kap. 4.4.3.

4.9 Certificate revocation and suspension | Zertifikatssperrung und Suspendierung

No stipulation.

Keine Vorgabe.

[TLS] The requirements listed below also apply to pre-certificates, if applicable.

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

4.9.1 Circumstances for revocation | Sperrgründe

In addition to the revocation reasons listed below, additional revocation reasons MAY be specified in the CPSs.

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

4.9.1.1 Reasons for revoking a Sub CA certificate | Gründe für die Sperrung eines Sub-CA Zertifikats

A Sub CA certificate SHALL be revoked if

- a written revocation request, even without giving reasons, has been made by the TSP,

Ein Sub-CA-Zertifikat MUSS gesperrt werden, wenn

- ein schriftlicher Sperrantrag, auch ohne Angabe von Gründen, vom TSP gestellt wurde,

- it is determined that the original certificate request was not authorized and cannot or should not be authorized retrospectively,
- it is determined that the private key of the Sub CA has been compromised or disclosed to an unauthorized person or organization or no longer complies with the requirements (see Section 6.1.5 and 6.1.6),
- it is determined that the certificate has been misused,
- it is determined that the Sub CA certificate has not been issued in compliance with this CP or that the operation is not in compliance with this CP,
- it is determined that any information in the certificate is incorrect or misleading,
- the operation of the Root CA or the Sub CA will be terminated and no arrangements have been made for the continuation of the revocation service,
- the right of the operator of the Root CA or Sub CA to issue certificates in accordance with the requirements of this CP expires or is revoked or terminated and no arrangements have been made for the continued operation of the revocation services.

When revoking a CA certificate, the best suitable revocation reason SHALL be set according to [RFC5280].

- 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 Reasons for revoking a subscriber certificate | Gründe für die Sperrung eines Endteilnehmer-Zertifikats

A certificate SHALL be revoked if

- an authorized revocation request, even without giving reasons, has been received from the subscriber or, if applicable, from the respective RA,
- relevant information in the certificate is not (or no longer) correct,
  Note: allowed deviations SHALL be described in the CPS.
- no authorization of the certificate exists (anymore), this includes:
  - information from the subscriber is available that the original application was not authorized and cannot or should not be authorized retroactively
  - [TLS] control over a FQDN or IP address specified in the certificate can no longer be trusted
  - [TLS] the use of a FQDN or IP address specified in the certificate is no longer allowed
  - [SMIME] domain authorization or mailbox control can no longer be relied upon
  - [SMIME] the use of an email address or FQDN specified in the certificate is no longer permitted
- a key weakness or compromise is demonstrated, this includes that the private key
  - has been given to an unauthorized person,
  - can be easily computed based on the public key (e.g., "debian weak key"),

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 (oder 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 im Zertifikat angegebene FQDN oder IP-Adressen 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,

- has been generated using a flawed method or methods are known to compromise the private key,
- no longer meets the requirements according to Sections 6.1.5 and 6.1.6,

- a violation of the CP, CPS or the Terms of Use is proven, this includes:
  - the certificate has not been issued in accordance with the relevant CPS
  - the certificate has been misused
  - [TLS] a wildcard certificate has been used to authenticate a fraudulently misleading Sub-FQDN
  - the subscriber has been suspended or revoked, as applicable

In addition, all affected certificates SHALL be revoked if

- the TSP ceases operation and has not taken precautions for continuing operation of the revocation services,
- the TSP loses the authorization to issue certain certificate types and has not taken precautions for continuing operation of the revocation services,
- the private key of a CA has been compromised or
- [QCP-l-qscd] [QCP-n-qscd] the certification of the QSCD used expires or the QCSDs have unacceptable security deficiencies.

When revoking a subscriber certificate, provided that the revocation reason is required, the correct revocation reason SHALL be selected as follows:

- `keyCompromise` SHALL be selected if the certificate subscriber's private key has been compromised.
  [TLS] [SMIME] `keyCompromise` MUST also be selected if the TSP becomes aware that the private key is potentially compromised, e.g. because it can be easily calculated based on the public key (e.g. Debian Weak Key) or the method used to generate the private key was flawed or a method exists that could expose the certificate subscriber's private key.
- `cessationOfOperation` SHALL be selected if the subscriber terminates the use of the certificate.
  [TLS] [SMIME] `cessationOfOperation` SHALL also be selected if the subscriber no longer has control over or is no longer authorized to use the domain names, IP addresses, or email addresses given in the certificate.
- `affiliationChanged` SHALL be selected if an attribute in the subjectDN or other data in the certificate has changed.
- `superseded` SHALL be selected if the certificate is replaced by a successor certificate and is no longer needed.
  [TLS] [SMIME] `superseded` SHALL also be selected if the CA becomes aware that the domain validation can no longer be relied upon, that the certificate was not issued in accordance with the relevant

- unter Verwendung einer mangelhaften Methode generiert wurde oder durch bekannte Methoden kompromittiert werden kann,
- 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` 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` 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` MUSS gewählt werden, wenn sich Attribute im subjectDN oder andere Daten im Zertifikat geändert haben.
- `superseded` 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

CPS, or that the certificate no longer meets the requirements of Section 6.1.5 and 6.1.6.

- `privilegeWithdrawn` SHALL be selected if the subscriber's right to use the certificate is withdrawn because, for example, the certificate request was not authorized, the certificate has been misused, or the subscriber has violated obligations.
  [TLS] [SMIME] `privilegeWithdrawn` SHALL also be selected if a wildcard certificate was used to authenticate a fraudulently misleading subordinate fully qualified domain name or the information in the certificate has changed significantly or is incorrect.

  NOTE: `privilegeWithdrawn` MAY be omitted from the list of revocation reasons selectable by certificate subscribers, since this revocation reason is set by the TSP.
- [SMIME] `certificateHold` SHALL be set when a certificate is suspended.

In all other cases, `unspecified` SHOULD be selected as the revocation reason.

[TLS] In all other cases, `unspecified` SHALL be selected as the revocation reason.

relevanten CPS erstellt wurde oder das Zertifikat nicht mehr den Anforderungen nach Kap. 6.1.5 und 6.1.6 genügt.

- `privilegeWithdrawn` 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.
- [SMIME] `certificateHold` MUSS gesetzt werden, wenn ein Zertifikat suspendiert 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 Who can request revocation | Berechtigte Sperrantragsteller

The revocation of a Sub CA SHALL always be requested by an authorized representative of the operator of the Sub CA. If one of the revocation reasons listed in Section 4.9.1.1 is identified by or reported to Telekom Security as operator of the Root CA, the revocation MAY also be initiated by Telekom Security without an existing revocation request.

[3145] The revocation of a Sub CA in the scope of TR-03145 is not in the scope of this CP, since the Sub CA certificates are not issued by a Telekom Root CA. The revocation of the Sub CAs SHALL be performed according to the specifications of the responsible operator of the Root CA and SHALL be described in the CPS.

The revocation of a subscriber certificate SHALL be requested by the subscriber himself or a responsible RA. If one of the reasons for revocation listed in Section 4.9.1.2 is identified or reported by a third party and is verified by the TSP, the revocation SHALL be initiated by the TSP. The further organizational and procedural requirements SHALL be described in the CPSs.

[QCP-n] [QCP-l] If a certificate contains information about a third party's power of representation or profession-related or other information pursuant to [VDG§12], the third party or the body responsible for the profession-

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

related or other information about the person MAY also request revocation if

- the power of representation or
- the prerequisites for the profession-related or other information on the person after being included in the qualified certificate

cease to exist.

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] In addition, subscriber certificates SHALL be revoked upon a justified request by the security officer.

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

4.9.3 Procedure for revocation request | Ablauf einer Sperrung

For revocation of certificates of all hierarchy levels, permanently available interfaces (7x24h) for submitting revocation requests or problem messages, that may lead to the revocation of certificates, as well as guidelines for using the interfaces, SHALL be provided.

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.

Revocation requests SHALL NOT be processed if they are not submitted by authorized applicants or are based on problem reports that are not verified as legitimate revocation reasons.

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.

The subscriber and, if different, the applicant SHALL be informed, if possible, of the revocation.

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

Revoked certificates SHALL NOT be unrevoked again.

Endgültig gesperrte Zertifikate DÜRFEN NICHT wieder entsperrt werden.

[VS-NfD] The processes for revoking certificates including the specified timelines SHALL be approved by the security officer.

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

4.9.4 Revocation request grace period | Fristen zur Beantragung einer Sperrung

As soon as a revocation reason according to Section 4.9.1 is determined, revocation SHALL be initiated immediately.

Sobald ein Sperrgrund gemäß Kap. 4.9.1 festgestellt wird, MUSS unverzüglich die Sperrung eingeleitet werden.

4.9.5 Time within which CA must process the revocation request | Fristen zur Verarbeitung von Sperranträgen durch die TSP

In addition to the time limits listed below, shorter time limits MAY be specified in the CPSs for certain revocation reasons.

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

Sub CA certificates SHALL be revoked within a reasonable period of time depending on the circumstances.

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

[TLS] [SMIME] Sub CA certificates SHALL be revoked within seven days after receipt of an authorized revocation request. This period includes the time to handover the revocation status to the certificate status services. After revocation of a Sub CA certificate, the corresponding entry in the CCADB SHALL be updated. If the revocation of the Sub CA certificate is required due to a security incident, the CCADB SHALL be updated within 24 hours, otherwise within 7 days.

[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.

Subscriber certificates SHALL be revoked as soon as possible, but no later than within 24 hours after receipt of an authorized revocation request. This period includes the time to handover the revocation status to the certificate status services.

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.

This does not apply to revocations requested for a later date, e.g., due to a planned termination of participation. In this case, the desired date for revocation of the certificate listed in the revocation request MAY be set as the date of receipt of the authorized revocation request, provided that this procedure is described in the CPSs.

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.

For revocations that are not based on authorized revocation requests but on other reasons for revocation listed in Section 4.9.1.2, the CPS SHALL specify the revocation periods.

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.

The TSP SHALL be able to respond to high-priority problem messages 24 hours a day and, if necessary, forward a message to law enforcement authorities and/or revoke the certificates affected by the problem.

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.

Within 24 hours of receipt of a problem report, the facts and circumstances SHALL be investigated and initial feedback on the findings available until then SHALL be provided to the subscriber and the reporting person. Subsequently, the results of the analysis SHALL be discussed with the subscriber and the reporting person and a decision SHALL be made as to whether a revocation is required.

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.

If revocation is required due to a problem report, the timing of revocation SHALL be determined, taking into account the requirements mentioned above and considering the following aspects:

- the nature of the alleged problem (scope, context, severity, extent, damage potential),
- the effects of revocation (direct and collateral effects on subscribers and relying parties),
- the number of problem messages for a certificate or subscriber,
- the entity that set the message,
- the relevant legislation.

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.

[TLS] [SMIME] Deviating from the generally defined revocation deadline of 24 hours, the following exceptions

[TLS] [SMIME] Abweichend von der grundsätzlich festgelegten Sperrfrist von 24 Stunden gelten folgende Ausnahmen: Zertifikate

apply: Certificates SHOULD be revoked within 24 hours and SHALL be revoked within 5 days if

- the method for generating the private key was faulty or a method exists that could expose the certificate subscriber's private key,
- the subscriber is no longer authorized to use the domain names, IP addresses or e-mail addresses specified in the certificate or the information in the certificate has changed significantly or is incorrect,
- the certificate was not issued in accordance with the relevant CPS or no longer meets the current requirements in accordance with Section 6.1.5 and 6.1.6,
- the certificate has been misused or the subscriber has violated obligations, or
- the TSP loses the right to issue certificates according to [BR] or [SBR].

However, the TSP SHALL also be able, in justified cases, to revoke certificates on a date specified by a Root Store operator that deviates from the above deadlines.

-

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.

-

If certificates cannot be revoked within the specified timeframe, the failure to revoke them in time SHALL be treated as a security incident.

Wenn Zertifikate nicht innerhalb der vorgegebenen Frist gesperrt werden können, MUSS die nicht fristgerechte Sperrung als Sicherheitsvorfall behandelt werden.

[TLS] [SMIME] Delayed revocations SHALL be reported as a "Revocation Delay Bug" in Bugzilla according to the CCADB policy.

[TLS] [SMIME] Nicht fristegrechte Sperrungen MÜSSEN als „Revocation Delay Bug“ in Bugzilla gemäß der CCADB-Policy gemeldet werden.

4.9.6 Revocation checking requirement for relying parties | Anforderungen an Zertifikatsnutzer zur Prüfung von Sperrinformationen

Relying parties SHOULD use the certificate status services according to Section 4.10 to check the status of certificates.

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

4.9.7 CRL issuance frequency

Certification Authority Revocation Lists (CARLs) SHALL be updated within 24 hours after revocation of a Sub CA certificate and regularly at least every 12 months.

Certificate Revocation Lists (CRL) SHALL be updated regularly at least every 24 hours.

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 SHALL also be updated following the revocation of a subscriber certificate in addition to the regular issuance.

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

4.9.8 Maximum latency for CRLs | Maximale Latenzzeit von Sperrlisten

No stipulation.

Keine Vorgabe.

4.9.9 On-line revocation/status checking availability | Verfügbarkeit von Online-Sperr-/Statusinformationen

See Section 4.10.

Siehe Kap. 4.10.

4.9.10 On-line revocation checking requirements | Anforderungen an Online-Überprüfungsverfahren

Relying parties should consider the OCSP response processing specifications in [RFC6960] when checking a certificate status via OCSP.

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

4.9.11 Other forms of revocation advertisements available | Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

No stipulation.

Keine Vorgabe.

4.9.12 Special requirements related to key compromise | Gesonderte Bedingungen bei Kompromittierung privater Schlüssel

No stipulation.

Keine Vorgabe.

[TLS] [SMIME] Accepted methods for evidence of key compromise SHALL be described in the CPSs in Section 4.9.12.

Regarding the reporting of suspected key compromise, see Section 1.5.2.

[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 Circumstances for suspension | Umstände für eine Suspendierung

Provided that suspension is allowed and offered, the circumstances for suspension SHALL be described in the CPS.

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

Sub-CA certificates SHALL NOT be suspended.

Sub-CA Zertifikate DÜRFEN NICHT suspendiert werden.

[TLS] Subscriber certificates SHALL NOT be suspended.

[TLS] Endteilnehmer-Zertifikate DÜRFEN NICHT suspendiert werden.

[3145] In addition to the revocation or suspension of certificates, subscriber SHALL also be suspended if it is

[3145] Ergänzend zur Sperrung oder Suspendierung von Zertifikaten MÜSSEN Zertifikatsnehmer suspendiert werden, wenn

determined that they are no longer fulfilling their obligations within the PKI, e.g., in the event of certificate misuse.	festgestellt wird, dass diese ihre Pflichten nicht mehr erfüllen, z.B. bei einem Zertifikatsmissbrauch.

4.9.14 Who can request suspension | Berechtigte Antragsteller für eine Suspendierung

No stipulation.	Keine Vorgabe.

4.9.15 Procedure for suspension request | Ablauf einer Suspendierung

No stipulation.	Keine Vorgabe.

4.9.16 Limits on suspension period | Begrenzung der Suspendierungsperiode

No stipulation.	Keine Vorgabe.

4.10 Certificate status services | Zertifikatsstatusdienste

At least for the validity period of all issued Sub CA and subscriber certificates, authentic and integrity-assured certificate status services SHALL be provided in the form of revocation lists and/or OCSP information.	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.
OCSP information SHOULD be provided for the subscriber certificates.	Zu den Endteilnehmer-Zertifikaten SOLLTEN OCSP-Auskünfte bereitgestellt werden.
[TLS] [SMIME] Revocation lists and OCSP information SHALL be provided for Sub CA and subscriber certificates, this also applies to pre certificates.	[TLS] [SMIME] Zu Sub-CA und Endteilnehmer-Zertifikaten MÜSSEN Sperrlisten und OCSP-Auskünfte bereitgestellt werden. Dies gilt auch für Pre-Zertifikate.
[QNCP-w] [QEVCP-w] Certificate status services SHALL be provided in integrity for at least two years beyond certificate validity.	[QNCP-w] [QEVCP-w] Die Zertifikatsstatusdienste MÜSSEN mindestens zwei Jahre über die Zertifikatsgültigkeit hinaus integer bereitgestellt werden.
[QCP-n] [QCP-l] Certificate status services SHALL be provided over the entire time of operation of the trust service. The integrity of the status information SHALL be guaranteed over the entire time period.	[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 Operational characteristics | Betriebliche Vorgaben

Certificate status services (revocation lists and OCSP) SHALL be time-synchronized (UTC) at least every 24 hours.	Zertifikatsstatusdienste MÜSSEN mindestens alle 24 Stunden zeitsynchronisiert (UTC) werden.
If revocation lists and OCSP information are provided, they SHALL be consistent after 24 hours at the latest, taking into account the different update times of both	Wenn Sperrlisten und OCSP-Auskünfte bereitgestellt werden, MÜSSEN diese unter Berücksichtigung der unterschiedlichen Aktualisierungsfristen beider Methoden spätestens nach 24 Stunden

methods. Differing update timelines, if any, SHALL be listed in the CPSs and a description SHALL be provided of how differing verification results are to be interpreted.

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 Operational characteristics for the provision of the OCSP responder | Betriebliche Vorgaben für die Bereitstellung der OCSP-Responder

The OCSP responders SHALL be operated in conformance with [RFC6960].

OCSP-Responder MÜSSEN konform zum [RFC6960] betrieben werden.

Concretizing to [RFC6960], requests for certificates with unknown certificate serial numbers SHALL NOT be answered with the status `good`.

Konkretisierend zum [RFC6960] gilt, dass Anfragen zu Zertifikaten mit nicht bekannten Zertifikatseriennummern NICHT mit dem Status good beantwortet werden DÜRFEN.

The response to be selected depends on the way the OCSP responder operates:

- For preproduced OCSP responses, such requests SHALL be answered with the error message `unauthorized`.
- For ad hoc generated OCSP responses such requests SHOULD be answered with the status unknown. They MAY also be answered with the status `revoked`, but then the extension `id-pkix-ocsp-extended-revoke` according to [RFC6960 #4.4.8] SHALL be set.

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. Sie DÜRFEN 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 requests for unassigned serial numbers SHOULD be logged.

OCSP-Anfragen zu nicht vergebenen Seriennummern SOLLTEN protokolliert werden.

OCSP responses MAY be cached and reused within their validity for further requests.

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

[TLS] OCSP responses to subscriber certificates SHALL be available within 15 minutes after generation of the certificate.

[TLS] OCSP-Antworten zu Endteilnehmer-Zertifikaten MÜSSEN innerhalb von 15 Minuten nach Erzeugung des Zertifikats verfügbar sein.

[TLS] [SMIME] OCSP responses to Sub CA certificates SHALL NOT exceed a maximum validity of 12 months. After a revocation of a Sub CA certificate, updated information SHALL be retrievable in the OCSP responder within 24 hours.

[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 responses to subscriber certificates SHALL have a validity of at least 8 hours but no more than 7 days. However, they SHALL NOT exceed the validity period of the issuing Sub CA certificate or the OCSP Signer certificate included in the `certs` attribute of the OCSP response.

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.

OCSP responses MAY be reused for further status requests for the certificate up to 4 hours after their generation, after which new responses SHALL be generated for further requests.

OCSP-Antworten DÜRFEN bis zu 4 Stunden nach ihrer Erzeugung für weitere Statusanfragen zu dem Zertifikat wiederverwendet werden, danach MÜSSEN auf weitere Anfragen neue Antworten generiert werden.

[QCP-n] [QCP-l] A validity end MAY be set.

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

4.10.1.2 Operational characteristics for the provision of revocation lists | Betriebliche Vorgaben für die Bereitstellung der Sperrlisten

All revocation lists SHALL be valid beyond the time of the next regular update.

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

The validity period of a last revocation list to the certificates in its scope SHALL be set to `99991231235959Z`.

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

Revoked certificates MAY in principle be removed from the CRLs after expiring, but they SHALL still be in the next regular CRL after their expiry date.

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 SHALL NOT exceed a validity of 12 months. CRLs SHALL NOT exceed a validity of 10 days.

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

[QCP] If CRLs and OCSP information are provided, expired certificates SHOULD NOT be removed from the revocation list. If only CRLs are provided, expired certificates SHALL NOT be removed from the CRLs.

[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.

If CRLs are provided, a final CRL SHALL NOT be issued until all certificates in its scope have expired or been revoked.

Wenn Sperrlisten bereitgestellt werden, DARF eine letzte Sperrliste NICHT ausgestellt werden, bevor alle Zertifikate in ihrem Anwendungsbereich abgelaufen oder gesperrt sind.

4.10.2 Service availability | Verfügbarkeit

The certificate status services SHALL be available 7x24h. In case of an incident, the greatest possible efforts SHALL be made to eliminate the incident within the specified service level agreements.

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] Sufficient capacity SHALL be provided to ensure that the response time does not exceed 10 seconds under normal operating conditions.

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

[3145] [NCP] The maximum downtime of the systems SHALL be specified in the CPSs.

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

4.10.3 Optional features | Optionale Merkmale

No stipulation.

Keine Vorgabe.

4.11 End of subscription | Kündigung durch den Zertifikatsnehmer

No stipulation.

Keine Vorgabe.

4.12 Key escrow and recovery | Schlüsselhinterlegung und Wiederherstellung

4.12.1 Key escrow and recovery policy and practices | Schlüsselhinterlegungs- und Wiederherstellungsrichtlinien und -Praktiken

If subscriber keys are escrowed, the subscribers SHALL be informed of this and the circumstances for escrow and recovery SHALL be described in the CPS.

Wenn Endteilnehmer-Schlüssel der hinterlegt werden, so MÜSSEN die Teilnehmer darüber informiert werden und es MÜSSEN die Umstände zur Hinterlegung und Wiederherstellung im CPS beschrieben werden.

4.12.2 Session key encapsulation and recovery policy and practices | Richtlinien und Praktiken zur Kapselung und Wiederherstellung von Sitzungsschlüsseln

No stipulation.

Keine Vorgabe.

5 Facility, Management an operational controls | Bauliche, organistaorische und betriebliche Regelungen

The approach to information security management SHALL be defined in an Information Security Policy approved by management and an appropriate information security management system (ISMS, e.g., following ISO 27001) SHALL be established that, among other things,

- manages the development, implementation and maintenance of security concepts including regular risk analyses for the Trust Services,
- inventories the assets (information as well as systems) and classifies it according to the risk management,
- is involved in change management for security-critical changes und
- includes regular auditing of the Trust Services.

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 Assets (Informationen und Systeme) 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.

The Information Security Policy SHALL be reviewed and communicated to all employees on a regular basis as well as when needed.

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

The inventories of assets SHALL comply with the requirements of the "NIS2[7]" Directive resp. the relevant implementing regulation and SHALL be reviewed on a regular basis as well as when needed.

Die Verzeichnisse der Assets MÜSSEN den Anforderungen der „NIS2[7]"-Richtlinie bzw. der relevanten Durchführungsverordnung genügen und regelmäßig sowie bei Bedarf revidiert werden.

The Information Security Policy SHALL also include provisions on the handling of risks related to information security in the supply chain ("Supply Chain Policy"), which also meet the requirements of the NIS2 Directive resp. the relevant implementing regulation and are reviewed on a regular basis as well as when needed.

Die Informationssicherheitsrichtline MUSS auch Regelungen zum Umgang mit Risiken bzgl. der Informationssicherheit in der Lieferkette („Supply Chain Policy") treffen, die ebenfalls den Anforderungen der NIS2-Richtlinie bzw. der relevanten Durchführungsverordnung genügen und regelmäßig sowie bei Bedarf revidiert werden.

Furthermore, the information security policy SHALL also include provisions regarding assets issued to employees or third parties in the event of a change or termination of employment or contract.

Darüber hinaus MUSS die Informationssicherheitsrichtline auch Regelungen bzgl. der an Mitarbeiter oder Dritte ausgegebene Assets bei Veränderung oder Beendigung des Arbeitsverhältnisses bzw. des Vertrags berücksichtigen.

The security concepts SHALL meet the following requirements:

- Protection of the confidentiality, integrity and availability of the certificate data and the certificate management process
- Protection against possible threats and hazards to the confidentiality, integrity and availability of certificate data and the certificate management process
- Protection against unauthorized or unjustified access, use, disclosure, substitution or destruction of

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.

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council | Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates

certificate data or the certificate management process
- Protection against loss or malicious destruction of certificate data or manipulation in the certificate management process
- Compliance with legally required security needs

- Schutz gegen Verlust oder mutwillige Zerstörung von Zertifikatsdaten oder Manipulationen im Zertifikatsmanagement-Prozess.
- Einhaltung von gesetzlich geforderten Sicherheitsanforderungen.

The security concepts SHALL in particular take into account the following aspects:
- Physical security (building and environment)
- Integrity protection of systems (including configuration management) and trusted code used
- Malware detection and prevention
- Network security and firewall management
- User and role management including the processes for assigning trusted roles
- Employee training, awareness and education
- Logical access control
- Logging
- Automatic locking of workstations in case of inactivity

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.

Risk analyses, that identify, analyze, and assess foreseeable internal and external threats that could lead to unauthorized access, disclosure, misuse, exchange, or destruction of certificate data or the certificate management process, SHALL be performed on an annual basis.

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.

The risk analyses SHALL consider the probabilities and potential damages of these threats, taking into account the sensitivity of the certificate data and the certificate management process, and assess the adequacy of the policies, procedures, information systems, technologies, and other precautions taken to address the threats.

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.

Based on the risk assessment, appropriate and adequate risk management measures (e.g., structural, organizational, personnel and state-of-the-art technical security measures) SHALL be developed and their implementation shall be managed and controlled by the ISMS.

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.

The risk assessment and any residual risks identified SHALL be approved by the management.

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

[VS-NfD] Before IT systems are used for VS-NfD, they SHALL be checked for compliance with the required classified security protection measures according to [VSA].

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

5.1 Physical controls | Physikalische Maßnahmen

In order to prevent loss, theft, damage, or compromise of assets, media, and information, physical measures SHALL be taken.

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

5.1.1 Site location and construction | Standort und Bauweise

Systems SHALL be operated in appropriate locations in secure premises with adequate physical protection. Potential natural disasters (e.g., floods) as well as disaster recovery SHALL be considered when selecting locations.

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.

If premises are shared with other organizations, the other systems SHALL be operated outside the area where the TSP's CA and status service systems are operated. The different areas SHALL be separated from each other by appropriate physical barriers.

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.

The TSP's systems MAY be operated in different security zones according to the criticality resulting from the risk assessment or the security requirements assigned. In particular, the Root CA's systems SHALL be operated in a high-security zone, separated from regular operations.

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] The instructions for the protection of VSIT rooms according to § 29 VSA [VSIT] SHALL be considered as guidance.

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

5.1.2 Physical access | Physikalischer Zutritt

Access to the rooms, where the TSP's systems are operated, SHALL be restricted to authorized persons in trusted roles via appropriate access controls. Where non-authorized persons require access to these rooms, they SHALL always be accompanied by an authorized person.

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.

The rooms where the TSP systems are operated SHALL have an intrusion alarm system to detect unauthorized entry.

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

The granted access authorizations SHALL be checked regularly.

Die erteilten Zutrittsberechtigungen MÜSSEN regelmäßig überprüft werden.

5.1.3 Power and air conditioning | Stromversorgung und Klimatisierung

Uninterruptible power supply as well as air conditioning of the systems according to the criticality resulting from the risk assessment as well as the agreed service levels SHALL be ensured.

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 Water exposures | Wassereinwirkung

The rooms in which components of the TSP are operated SHALL be protected from water exposure according to the criticality resulting from the risk assessment.

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 Fire prevention and protection | Brandvorsorge und Brandschutz

The rooms in which components of the TSP are operated SHALL be protected against destruction by fire according to the criticality resulting from the risk assessment.

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 Media storage | Aufbewahrung von Medien

Measures SHALL be taken to protect against accidental use outside the secured environment, damage, theft, unauthorized access, and obsolescence of the relevant TSP media. These measures SHALL take into account the retention period of the media. All media SHALL be handled securely according to the classification of the information stored on it.

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 Waste disposal | Abfallentsorgung

In order to prevent unauthorized use or access to information, secure disposal processes SHALL be established. In particular, media containing sensitive data SHALL be disposed of securely when no longer needed.

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 Off-site backup | Externe Sicherung

No stipulation.

Keine Vorgabe.

5.2 Procedural controls | Organisatorische Maßnahmen

5.2.1 Trusted roles | Vertrauenswürdige Rollen

To ensure secure operation, the TSP SHALL have an appropriate organization that includes at least the following trusted roles:

- Head of Trust Center: has the overall responsibility for the services of the TSP and reports to the management of Telekom Security

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 und berichtet an die Geschäftsführung der Telekom Security

- Head of qTSP: is the contact and information person for the national supervisory authorities for the qualified Trust Services
- Solution Manager: is responsible for and manages a Trust Service
- Trust Center Information Security Officer: has overarching responsibility for the Trust Center's Information Security Policy as well as the implementation of security controls and reports to the Head of Trust Center
- Registration staff/Validation Specialist: reviews and processes applications for certificate-issuance, -suspension, -revocation or -renewal
- System-Administrator, -Operator: installs, configures and maintains the systems, can perform backups and restores of data
- Internal Auditor: checks for example log data, databases and paper-based documentation of the Trust Services on a regular basis as well as in case of discrepancies
- Compliance Manager: regularly reviews the requirements underlying the Trust Services, coordinates these with the Solution Managers and coordinates the necessary audits by external auditors.

- 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 Informationssicherheitsrichtlinie des Trust Center sowie die Implementierung von Sicherheitsmaßnahmen und berichtet an den Leiter Trust Center
- Registrierungsmitarbeiter/Validierungsspezialist: prüft und bearbeitet Anträge zur Zertifikatsausstellung, -suspendierung, -sperrung oder -erneuerung
- System-Administrator, -Operator: installiert, konfiguriert und wartet die Systeme, kann Daten-Sicherungen und -Rücksicherungen durchführen
- 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.

The relevant roles including an overview of the assigned activities SHALL be described in the CPSs.

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

5.2.2 Number of persons required per task | Anzahl der für eine Aufgabe erforderlichen Personen

At least one substitute SHALL be appointed for all roles listed in Section 5.2.1.

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

Security-relevant or -critical activities, such as generation, backup and recovery of CA keys, SHALL be performed in dual control by persons in trusted roles. The number of employees performing such security-relevant or -critical activities SHALL be kept to a minimum.

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.

The security-relevant and -critical activities for which a dual control principle (or more) is required SHALL be described in the CPSs.

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

[EVCP] Certificate applications SHALL be validated and approved using the dual control principle, see Section 4.2.1. In order to ensure the dual control principle, auditable security controls SHALL be implemented.

[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 Identification and authentication for each role | Identifizierung und Authentifizierung für vertrauenswürdige Rollen

The identification of suitable persons to fill roles, the transfer of roles, and their withdrawal SHALL follow a documented process.

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

Role owners SHALL be officially appointed to the trusted role by the management of the TSP.

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

Prior to the delegation of a trusted role, acceptance to the delegation of the role and its associated responsibilities, as well as the resulting duties to ensure security, SHALL be obtained from the individual to whom the role is to be delegated.

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.

Furthermore, it SHALL be ensured that no conflicts of interest arise from the assignment of a role and that independence is maintained, i.e., that

- the areas entrusted with generating and revoking certificates SHALL be independent of other organizations in their decisions to establish, provide, maintain, and suspend Trust Services in accordance with applicable certificate policies,
- that all employees involved in certificate generation and revocation SHALL be free from financial or other pressures in the performance of their tasks that could affect trust in the Trust Services. This applies to all employees in trusted roles as well as senior managers and executives.

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.

The structure that ensures impartiality of operation SHALL be documented.

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

Role owners SHALL be made aware that they may only act in the assigned role when performing tasks assigned to the role.

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

The assignment of the required permissions SHALL follow the "least privilege" principle, i.e., all permissions SHALL be limited to the required minimum.

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

Upon termination of employment or a change of activity of an employee in a trusted role, its access privileges SHALL be adjusted or revoked within 24 hours.

Nach Beendigung des Arbeitsverhältnisses oder einem Wechsel der Tätigkeit eines Mitarbeiters in einer vertrauenswürdigen Rolle MÜSSEN dessen Zugriffsberechtigungen innerhalb von 24 Stunden angepasst bzw. entzogen werden.

If trusted roles or parts thereof are transferred to third parties (e.g., external RAs, see Section 1.3.2), responsibilities and regulations SHALL be clearly defined and corresponding agreements SHALL be made to ensure that all regulations specified by the TSP are also complied with by the third parties.

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 Roles requiring separation of duties | Rollen, die eine Aufgabentrennung erfordern

Conflicting duties and responsibilities SHALL be separated from each other.

The following roles SHALL be separated:
- Head of Trust Center and/or Head of TSP
- Trust Center Information security officer and/or internal auditor
- Registration staff
- Administrator

In addition, the persons in the roles above SHALL NOT also be applicants for subscriber certificates. Exceptions to this are
- applications for the TSP's own certificates and certificates for the TSP's employees,
- applications for an organization's own certificates that operates an external RA, as well as certificates for that organization's employees.

Exceptions SHALL be described in the CPSs.

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 Personnel controls | Personelle Maßnahmen

5.3.1 Qualifications, experience, and clearance requirements | Qualifikationen, Erfahrung und Freigaben

The management of the TSP SHALL have
- experience or training related to the Trusted Services,
- familiarity with security procedures for personnel with security responsibilities, and
- experience with information security and risk assessment sufficient to perform management functions.

TSP employees SHALL have sufficient expert knowledge and qualifications to perform their tasks based on their experience and/or appropriate training. The required skills and experience MUST be documented.

In addition, the employees SHALL be adequately trained on general security and data protection regulations as well as the specific requirements of the TSP's ISMS for the performance of their tasks.

TSP employees involved in the verification of identity documents as part of the identification process SHALL be trained in the appearance and validation of accepted

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. Die erforderlichen Fähigkeiten und Erfahrungen MÜSSEN dokumentiert werden.

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

identity documents and have access to relevant sources of information.

akzeptierten Identitätsdokumente geschult sein und Zugang zu einschlägigen Informationsquellen haben.

5.3.2 Background check procedures | Verfahren zur Hintergrundprüfung

Before hiring a person, their identity and trustworthiness SHALL be verified.

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

[EVCP] Identification of persons to be entrusted with a trusted role SHALL be done face-to-face and by presenting an official identification document and a background check SHALL be done, that includes checking of
- previous employment,
- professional references,
- educational qualifications, and
- an official certificate of good conduct.

[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] The reliability of personnel SHALL be verified by regular submission of official certificates of good conduct.

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

[3145] It SHALL be ensured that individuals, who are to be entrusted with critical or security-related processes have successfully completed a security check. If the security check reveals that a person has been convicted to a crime, that affects his suitability for the intended role, that person SHALL NOT be entrusted with that role.

[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] The above-mentioned security check according to [3145] SHALL be done according at least to [SÜG] level “Ü1”.

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

5.3.3 Training requirements | Schulungsanforderungen

See Section 5.3.1.

Siehe Kap. 5.3.1.

[TLS] [SMIME] All registration staff SHALL be trained on the following topics:
- basic knowledge of PKI, authentication and verification policies and procedures
- common threats to the information verification process, including phishing and social engineering
- relevant CP and CPSs as well as the [BR], [SBR] and the [EVCG], if applicable.

Evidence of these trainings SHALL be kept and it SHALL be documented that each employee involved in validation has the required know-how before taking on the activities.

In addition, registration staff SHALL be required to pass an examination provided by the TSP on the information

[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],

verification requirements outlined in the [BR], [SBR] and the [EVCG], if applicable.

[SBR] und ggf. [EVCG] aufgeführten Anforderungen zur Validierung von Informationen bestehen.

5.3.4 Retraining frequency and requirements | Nachschulungsintervalle und -anforderungen

Personnel SHOULD be trained regularly (at least annually) on current threats and security practices.

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

Through appropriate regular training SHALL be ensured, that personnel in trusted roles maintain the required know-how at all times.

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

5.3.5 Job rotation frequency and sequence | Häufigkeit und Abfolge der Arbeitsplatzrotation

No stipulation.

Keine Vorgabe.

5.3.6 Sanctions for unauthorized actions | Sanktionen bei unbefugten Handlungen

Personnel SHALL be accountable for their actions. Appropriate sanctions SHALL be imposed when violating the requirements of the TSP.

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

5.3.7 Independent contractor requirements | Anforderungen an unabhängige Auftragnehmer

The requirements listed in Section 5.3 apply by analogy to third parties assigned by the TSP, if applicable.

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

[TLS] [SMIME] Third party personnel involved in the issuance of certificates SHALL be checked for compliance with the training and qualification requirements according to Sections 5.3.1 and 5.3.3.

[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 über-prüft werden.

5.3.8 Documentation supplied to personnel | Dem Personal bereit gestellte Dokumentation

Role owners SHALL be provided with role descriptions that describe the responsibilities and duties resulting from the respective role, taking into account the requirements listed above (Section 5.3).

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

Where required, the role descriptions SHALL differentiate between general and specific roles.

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

The security roles and responsibilities defined in the information security policy SHALL be described in job descriptions or in documents available to all affected employees.

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 Audit logging procedures | Protokollierungsverfahren

5.4.1 Types of events recorded | Zu protokollierende Ereignisse

The following events including the precise time, the identity of the trigger (if applicable) and the description of the event SHALL be logged in the respective system logs:

- All significant events of the certificate and key management systems as well as status services, which are at least (if applicable)
  - key generation, backup, storage, recovery, archiving and destruction,
  - certificate application including renewal,
  - validations, approvals and rejections,
  - issuance of certificates,
  - certificate revocation application,
  - revocation of certificates,
  - generation of revocation lists,
  - OCSP requests and
  - signing of OCSP responses.
- All security relevant events on the PKI and security systems, in particular
  - changes to the systems' security policies,
  - system startup and shutdown,
  - system crashes and hardware failures,
  - time synchronization events,
  - firewall and router activities and
  - successful and unsuccessful PKI system access attempts.
- Installation, update and deinstallation of software on the PKI systems.

In addition, all physical entries and exits to/from the security zones SHALL be logged in the access systems.

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,
  - OCSP-Anfragen 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 Frequency of processing log | Häufigkeit der Log-Verarbeitung

Log data SHALL be evaluated as follows:

- Security relevant events SHALL be evaluated as described in Section 6.6.2.
- All other records SHALL be evaluated, when necessary, e.g. for troubleshooting or analysis activities.

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 Retention period for audit log | Aufbewahrungszeitraum für Logdaten

Log data SHALL be retained for a reasonable period of time. The retention periods SHALL be described in the CPSs, see also Section 5.5.2.

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

[TLS] [SMIME] Log data SHALL be retained for at least two years after its occurrence.	[TLS] [SMIME] Die Logdaten MÜSSEN für mindestens zwei Jahre nach ihrem Eintreten aufbewahrt werden.

5.4.4 Protection of audit log | Schutz der Audit-Protokolle

Log data SHALL be kept confidential, integrity-secured and protected in such a way that they cannot be easily destroyed or deleted, see also Section 5.4.6. It SHALL be described in the CPSs how the protection of these records is ensured.	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.
Log data SHALL be made available in case of need, e.g., in legal proceedings or upon request of internal and external auditors.	Logdaten MÜSSEN im Bedarfsfall bereitgestellt werden, z.B. in Gerichtsverfahren oder auf Anfrage interner und externer Auditoren.
Log data retention SHALL be monitored (e.g., in internal audits).	Die Aufbewahrung der Logdaten MUSS überwacht werden (z.B. in internen Audits).

5.4.5 Audit log backup procedures | Backup-Verfahren für Audit-Protokolle

No stipulation.	Keine Vorgabe.

5.4.6 Audit collection system (internal vs. external) | Audit-Sammelsystem (intern vs. extern)

Log data SHALL be collected in a separate tamper-proof system, i.e., not only in the system where the events are logged.	Die Logdaten MÜSSEN in einem separaten manipulationssicheren System, d.h. nicht nur in dem System, in dem die Ereignisse protokolliert werden, gesammelt werden.
The system SHALL be designed in such a way that entries can only be added but not deleted during the specified retention period, the storage capacity of the system SHALL be designed accordingly.	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 Notification to event-causing subject | Benachrichtigung der Person, die ein Ereignis ausgelöst hat

No stipulation.	Keine Vorgabe.

5.4.8 Vulnerability assessments | Nutzung von Protokolldaten zur Schwachstellenprüfung

No stipulation.	Keine Vorgabe.

5.5 Records archival | Aufbewahrung von Aufzeichnungen

5.5.1 Types of records archived | Aufzubewahrende Aufzeichnungen

For each certificate, the application/certificate history SHALL be recorded, including date, time and, if applicable, the identity of the acting person. This includes the following activities of subscribers as well as internal and, if applicable, external RAs:

- all activities related to the application, registration, validation and approval or rejection of applications for issuance, renewal and revocation of certificates of all hierarchy levels
- all activities related to the lifecycle of keys and certificates of all hierarchy levels. This includes at least, if applicable,
  - the generation, storage, backup, recovery, archiving and destruction of keys, including the preparation or provision of QSCD or other cryptographic devices, and
  - the issuance, acceptance, publication and revocation of certificates.

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.

Furthermore, for each certificate, the relevant information and documents submitted by the applicant or provided to the applicant as part of the application for issuance, renewal, modification or revocation SHALL be recorded resp. retained ("registration information"). This shall include at least

- the information regarding the identity and other attributes, if any, of the subscriber, including, if applicable, a reference to the documents or sources used for verification.
  Note: If the identity or attributes were verified against a public and permanently accessible source, information on which source was used and whether the data matched is sufficient. An extract from the source does not have to be kept.
- the agreement concluded with the subscriber, if any, but at least acceptance of the Terms of Use in force at the time of application.

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

[SMIME] In the case of TSP-Ident, in addition to the above records, the issuer, validity period and unique number of the verified identity document SHALL be recorded.

[SMIME] 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.

In addition, the following information and documents SHALL be recorded resp. retained:

- all published CP, CPS, and Terms of Use
- certification documents and audit reports
- relevant documentation related to the security of the systems from the
  - change management,
  - vulnerability management,
  - role management,
  - lifecycle management of cryptographic modules

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.

- if applicable, other information required to ensure continuity of services or needed as evidence in legal proceedings.

Taking into account the relevant privacy aspects, additional data MAY be recorded. In the CPSs and Terms of Use SHALL be described which data are recorded.

[TLS] [SMIME] For each certificate, the method used to validate the domain name, IP address or email address according to [BR#3.2.2.4], [BR#3.2.2.5] or [SBR#3.2.2] including the version of the [BR] resp. [SBR] on which the validation was based, SHALL also be recorded.

[3145] Records SHALL be archived in such a way that all certificates can be uniquely assigned to a registered subscriber. In addition, tracking SHALL be possible to prevent fraudulent or manipulated certificates from being generated.

- 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 Retention period for archive | Aufbewahrungszeitraum für Aufzeichnungen

In addition to the certificates themselves, the following of the records listed in Section 5.5.1 SHALL be archived for at least 7 years after the expiration of the validity of the affected certificates:

- Application/certificate history
- Registration information
- CP, CPS and Terms of Use
- Certification documents and audit reports

All other records SHALL be retained for a minimum of 2 years.

The retention period (if applicable per certificate type) SHALL be described in the CPSs as well as in the Terms of Use.

The obligation to retain records also applies beyond the termination of a Trust Service. The termination plan SHALL therefore specify which information is transferred where and how this information can be accessed, see also Section 5.8.

[QCP-l] [QCP-n] The certificate history and registration information SHALL be kept permanently.

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 Protection of archive | Schutz der Aufzeichnungen

Records SHALL be maintained in confidence, with integrity, and protected from destruction or deletion.

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

[EVCP] Retention of information and documents SHALL be monitored (e.g., in internal audits).

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

[QCP] Electronically retained records that are integrity-secured using QES or time stamps SHALL be re-protected by appropriate measures to ensure long-term preservation of evidence if the previous protection weakens over time.

[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 Archive backup procedures | Backup-Verfahren für Aufzeichnungen

No stipulation.

Keine Vorgabe.

5.5.5 Requirements for timestamping of records | Anforderungen an Zeitstempel von Datensätzen

No stipulation.

Keine Vorgabe.

5.5.6 Archive collection system (internal or external) | Archivsystem (intern oder extern)

No stipulation.

Keine Vorgabe.

5.5.7 Procedures to obtain and verify archive information | Verfahren zur Beschaffung und Überprüfung von Aufzeichnungen

Archived information SHALL be evaluated and made available when needed, e.g., in case of problem reports, in legal proceedings, or upon request of internal and external auditors.

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

Access to the archived information SHALL be defined and documented internally within the TSP.

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

5.6 Key changeover | Schlüsselwechsel

Prior to the expiration of a CA certificate, a new CA certificate SHALL be issued in good time in accordance with the current versions of this CP and the CPSs, provided that the affected Trust Service is to be continued. In doing so, the period between the publication of the new CA certificate and the taking out of service of the expiring CA certificate SHOULD be sufficiently long so that there is no interruption in operation for the subscribers.

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 Compromise and disaster recovery | Kompromittierung und Notfall-Wiederherstellung

5.7.1 Incident and compromise handling procedures | Verfahren zur Meldung und Behandlung von Vorfällen und Kompromittierungen

The procedures for notification and handling of incidents and compromises and for recovery from outages or disasters SHALL be described in the emergency documentation.

Incident and Emergency documentation SHALL include the following aspects:

- emergency prevention:
  - requirements to back up critical cryptographic material at another location
  - requirements to regularly back up all relevant data needed to reestablish CA operations after a disaster at secure, preferably remotely located sites, this also includes the integrity check of the backups as well as regular documentes recovery tests
  - distance from the primary site to sites that can be used to reestablish CA operations
- naming of all roles involved and escalation levels
- responsibility of all parties involved
- guidelines for the assessment and classification of events, as well as reassessment and reclassification in light of new information
- conditions under which an incident becomes an emergency
- emergency processes
- fallback processes
- recovery processes
- processes for reporting
  - security breaches to the supervisory authorities (within 24 hours) or other relevant stakeholders,
  - security breaches that disadvantageously affect natural persons or organizations to the affected persons or organizations (without delay),
  - privacy incidents to the responsible authorities or other relevant stakeholders (within 24 hours)
- processes for the optional involvement of the BSI[8] in its role as a national CSIRT to support emergency or crisis situations
- recovery time targets
- follow-up incl. root cause analysis to avoid recurrence
- review cycles of the emergency plan (at least annually)
- awareness and training requirements
- regular emergency exercises (at least annually)

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

Die Vorfall- und 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, dazu zählen auch die Integritätsprüfung der Backups sowie regelmäßige dokumentierte Wiederherstellungstests,
  - Entfernung des Hauptstandorts zu den Standorten, die zur Wiederherstellung des Geschäftsbetriebs genutzt werden können,
- Benennung aller beteiligten Rollen und Eskalationsstufen,
- Verantwortung aller Beteiligten,
- Vorgaben zur Bewertung und Klassifizierung von Ereignissen sowie Neu-Bewertung und -Klassifizierung bei neuen Erkenntnissen,
- 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),
- Prozesse zur optionalen Einbindung des BSI[8] in dessen Rolle als nationales CSIRT zur Unterstützung bei Notfall- oder Krisensituationen,
- Zielvorgaben für die Wiederherstellungszeit,
- Nachbereitung inkl. Ursachenermittlung zur Vermeidung von Wiederholungen,
- Review Zyklen des Notfallplans (mindestens jährlich),

[8] Federal Office for Information Security | Bundesamt für die Sicherheit in der Informationstechnik

- plan for resuming operations after interruption or failure of critical business processes
- establishment of acceptable downtime and recovery times
- procedures for securing the impacted site to the maximum extent possible during the period following a disaster and prior to recovery at the original site or at another site

- 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.

The emergency documentation SHALL be disclosed to auditors upon request.

Die Notfalldokumentation MUSS den Auditoren auf Anfrage offengelegt werden.

Procedures for notifying incidents SHALL be established and it SHALL be ensured that they are known and used by employees.

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

In order to minimize potential damage, it SHALL be responded in a timely manner to incidents reported by individuals and alarms reported by systems (see Section 6.6.2). Potentially security-critical incidents SHALL be investigated immediately by personnel in trusted roles.

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] The emergency documentation SHALL include a plan for certificate mass revocation in accordance with [BR#5.7.1.2]. Mass revocations SHALL be tested annually in accordance with the plan, and the results of the tests SHALL be incorporated into the plan for continuous improvement.

[TLS] Die Notfalldokumentation MUSS einen Plan gemäß [BR#5.7.1.2] für Massensperrungen von Zertifikaten enthalten. Massensperrungen MÜSSEN jährlich gemäß den Vorgaben des Plans getestet werden, die Ergebnisse der Tests MÜSSEN im Sinne der kontinuierlichen Verbesserung in den Plan einfließen.

[TLS] [SMIME] Violations of the relevant Root Store Policies SHALL be immediately reported to the appropriate Root Store operators and issuance of the affected certificate types SHOULD be stopped until the cause of the violation is resolved.

[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] The emergency plan SHALL be approved by the security officer.

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

5.7.2 Computing resources, software, and/or data are corrupted | Wiederherstellung bei Beschädigung von Computern, Software oder Daten

See Section 5.7.1.

Siehe Kap. 5.7.1.

5.7.3 Entity private key compromise procedures | Verfahren bei Kompromittierung von privaten Schlüsseln

Compromise, suspected compromise, and loss of a CA private key SHALL be defined as an emergency in the emergency documentation and the resulting activities SHALL be described.

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.

In the event of a CA key compromise, the corresponding CA certificate SHALL be revoked and all affected parties (subscribers as well as all others with whom the TSP has agreements) SHALL be informed. In addition, the information SHALL be made available to relying parties and it SHALL be indicated that the certificates and status information issued by the affected CA no longer can be trusted.

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.

Furthermore, all subscriber certificates SHOULD be revoked.

Des Weiteren SOLLTEN alle Endteilnehmer-Zertifikate gesperrt werden.

[QCP] The procedures for providing status information on subscriber certificates in case of compromise of a CA key SHALL be described in the CPS.

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

[3145] In the event of a suspected compromise of a CA key, the affected key SHALL not be used until final clarification.

[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 Business continuity capabilities after a disaster

In the event of an emergency, operations SHALL be reinstated within the time period specified in the emergency documentation after all causes have been eliminated by appropriate mitigation measures.

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 CA or RA termination

When terminating a Trust Service, potential disruptions for subscribers and relying parties SHALL be minimized as far as possible.

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

If possible, arrangements SHOULD be made to allow customers to transition to the use of comparable Trust Services from another TSP..

Sofern möglich, SOLLTEN Vorkehrungen getroffen werden, um den Kunden einen Übergang zur Nutzung vergleichbarer Trust Services eines anderen TSP zu ermöglichen.

Prior to termination of a Trust Service, the following SHALL be done:

- All affected parties (subscribers, relevant supervisory authorities if any, affected Root Store operators or other affected parties with whom the TSP has contracts) are informed,
- Relying parties are provided with the information about the termination or transfer,
- Agreements with subcontractors, e.g., external RAs, are terminated.
- A reliable organization is obligated to retain all information necessary to demonstrate the operation of the TSP for a reasonable period of time, as agreed upon with subscribers and others, if applicable. At a minimum, this includes
  - registration information,

Vor der Beendigung 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.
- 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

- certificate status information,
- event log archives,
- CA certificates.

- The private CA keys are destroyed or taken out of service in such a way that they cannot be reused.
- All certificates that are still valid and not yet revoked are revoked.

Upon termination of a Trust Service and transfer of the information to another entity, all keys, certificates and customer data SHALL be deleted.

The arrangements made to terminate a Trust Service SHALL be defined in a maintained termination plan.

Furthermore, the CPS SHALL describe how to proceed in case of termination of a Trust Service, at a minimum this includes

- the information of all affected parties,
- the handling of status information on unexpired certificates, and
- if applicable, the transfer of duties to others.

[QCP] The CPS SHALL also describe the procedures for providing status information for all expired certificates in accordance with Section 4.10.

[QCP-l] [QCP-n] The termination plan SHALL take into account,

- that the subscribers are informed, as far as possible, two months in advance about the termination and the transfer of the certificates,
- that all certificates, their status information as well as the relevant information according to Section 5.5.1 are handed over, if possible, in electronic form according to the state of the art, either to another qualified TSP or to the Federal Network Agency as the responsible supervisory authority.

`cessationOfOperation` SHALL be specified as the revocation reason for the revoked certificates in the status services.

Prior to the termination of an RA, it SHALL be defined and described in the CPS, which information (e.g., certificate applications kept or archived at the RA or other registration information) must be handed over to the TSP.

- 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.

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

Die Vorkehrungen, die zur Beendigung 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 Technical security controls | Technische Sicherheitsmaßnahmen

6.1 Key pair generation and installation | Generierung und Installation von Schlüsselpaaren

6.1.1 Key pair generation | Generierung von Schlüsselpaaren

All keys SHALL comply with the algorithms, key lengths and quality requirements listed in Sections 6.1.5 and 6.1.6.

Alle Schlüssel MÜSSEN den in Kap. 6.1.5 und 6.1.6 aufgeführten Algorithmen, Schlüssellängen und Qualitätsanforderungen genügen.

The keys SHALL be considered suitable for the entire lifetime and intended uses at the time of generation.

Die Schlüssel MÜSSEN für die gesamte Lebensdauer und die beabsichtigten Verwendungszwecke zum Zeitpunkt der Generierung als geeignet angesehen werden.

6.1.1.1 Generierung von CA-Schlüsselpaaren

CA key pairs SHALL be generated in a crypto module according to Section 6.2.1 in the secure environment of the Trust Center as part of a key ceremony, it SHALL be the crypto module in which the private key will be used later, so that no import or export of the keys is required except for backup purposes.

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.

The roles involved as well as their tasks and responsibilities before, during and after the key ceremony SHALL be defined and documented.

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

The individual steps of the key ceremony SHALL follow a defined protocol and be documented within it.

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

Generation SHALL be performed by at least two Trust Center employees acting in trusted roles.

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

The following requirements apply for the generation of Root CA keys:

- Each of the two employees SHALL have knowledge only of a part of the activation data required for key generation.
- The two employees SHALL act in different roles.

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.

The following requirements apply for the generation of Sub CA keys:

- To prove authenticity and integrity, the hash value of the generated public key or of the CSR containing the public key SHALL be included in the generation protocol and handed over during certificate application (see Section 4.1).

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.

An internal auditor (see Section 8.2) SHALL monitor the key ceremony and confirm its correct performance in the protocol.

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

[TLS] [SMIME] Both an internal and a qualified external auditor (see Section 8.2) SHALL monitor the key ceremony and confirm its correct execution in the protocol.

[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.

[QCP] Key ceremonies for Root CAs SHALL be monitored by both an internal and a qualified external auditor (see chapter 8.2) and their correct execution SHALL be confirmed by both in the protocol.

[QCP] Schlüsselzeremonien für Root-CAs MÜSSEN sowohl von einem internen als auch von einem qualifizierten externen Auditor (siehe Kap. 8.2) überwacht werden und deren korrekte Durchführung MUSS von beiden im Protokoll bestätigt werden.

6.1.1.2 Generierung von OCSP-Signer-Schlüsselpaaren

OCSP Signer key pairs SHALL be generated in cryptographic modules according to Section 6.2.1, it SHALL be the crypto module in which the private key will be used later, so that no import or export of the keys is required except for backup purposes.

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 key pairs SHALL be generated in cryptographic modules according to Section 6.2.1.

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

6.1.1.4 Generierung von Endteilnehmer-Schlüsselpaaren

Subscriber key pairs MAY be generated either by the TSP, a delegated third party or the subscriber itself.

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

If the keys are generated by the subscribers, the subscribers SHALL be informed about the permitted algorithms and key lengths to be used.

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

If the keys are generated by the TSP, the keys SHALL be generated in a secure manner and SHALL be maintained until certificate generation, ensuring integrity and confidentiality.

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] Subscriber keys SHALL NOT be generated by the TSP.

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

[QCP-n-qscd] [QCP-l-qscd] Subscriber key pairs SHALL be generated by a certified QSCD (see Section 6.2.1).

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

[3145] If subscriber keys for cryptographic token as a storage medium of the keys are generated by the TSP, the

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

keys SHOULD be generated by the token itself. Keys generated outside the token SHALL be deleted immediately after they are stored in the token unless a backup of the subscriber keys is provided.

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 Private key delivery to subscriber | Bereitstellung der privaten Schlüssel an die Zertifikatsnehmer

The procedures for handing over the keys SHALL be described in the Terms of Use and the CPSs.

If subscriber keys are generated by the TSP, the following requirements SHALL be considered:

- The keys SHALL be handed over to the subscriber in such a way that the preservation of confidentiality and integrity is ensured and unauthorized use is impossible unless the TSP manages the keys on behalf of the subscriber.
- After the keys have been handed over to the subscriber, all copies of the keys SHALL be deleted from the TSP's systems, unless the keys are to be escrowed with the TSP on behalf of the subscriber (see Section 6.2.3).

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.
- 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).

[QCP-n-qscd] [QCP-l-qscd] The private keys SHALL be handed over to the subscribers in certified QSCDs according to Section 6.2.1.

[QCP-n-qscd] [QCP-l-qscd] Die privaten Schlüssel MÜSSEN den Zertifikatsnehmern in zertifizierten QSCD gemäß Kap. 6.2.1 übergeben werden.

[3145] The procedures for issuing tokens SHALL be described in the terms of use and the CPSs.

If the TSPs generate the keys for the subscriber certificates, it SHALL be ensured that

- the keys are delivered to the correct recipient,
- the confidentiality of the keys is guaranteed during delivery,
- keys are deleted in the systems of the TSPs after delivery to the correct recipient.

[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.

[SMIME] When subscriber key pairs are generated by the TSP or a delegated third party, the private keys SHALL NOT be stored in clear text.

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

6.1.3 Public key delivery to certificate issuer | Übergabe öffentlicher Schlüssel an die TSP

No stipulation.

Keine Vorgabe.

[TLS] Formats and methods of accepted CSRs SHOULD be specified in the CPSs or in documents referenced by the CPSs.

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

6.1.4 CA public key delivery to relying parties | Bereitstellung der öffentlichen CA-Schlüssel

CA certificates SHALL be made accessible to the general public in an authentic and integrity-protected form (see Section 2.2).

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

For Root CA certificates, additional validation mechanisms SHALL be provided, such as a validation option of the hash value of the certificate against a trusted source.

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 Key sizes | Schlüssellängen

The keys of all certificates SHOULD meet the requirements from [SOGIS].

Schlüssel aller Zertifikate SOLLTEN den Anforderungen aus [SOGIS] genügen.

[ETSI] The keys of all certificates SHALL meet the requirements from [ETS312].

[ETSI] Die Schlüssel aller Zertifikate MÜSSEN den Anforderungen von [ETS312] genügen.

Accordingly, the following minimum requirements SHALL be applied:

- RSA: Keys SHOULD have a length of at least 3,000 bits (recommendation according to [SOGIS]). Keys with a length of more than 1,900 bits and less than 3,000 bits MAY still be used until 2028 (Legacy according to [ETS312]).
- ECC: Keys from the following curves SHOULD be used (recommendation according to [SOGIS]):
  - BrainpoolP256r1
  - BrainpoolP384r1
  - BrainpoolP512r1
  - NIST P-256
  - NIST P-384
  - NIST P-521

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 2028 verwendet werden (Legacy gem. [ETS312]).
- ECC: Es SOLLTEN Schlüssel aus folgenden Kurven verwendet werden (Recommendation gem. [SOGIS]):
  - BrainpoolP256r1
  - BrainpoolP384r1
  - BrainpoolP512r1
  - NIST P-256
  - NIST P-384
  - NIST P-521

If the key lengths used are no longer sufficient for the intended use due to new knowledge or requirements, the subscribers and relying parties SHALL be informed and a schedule SHALL be set to revoke the certificates and migrate to sufficiently long keys.

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] The following requirements apply to RSA keys additionally:

- They SHALL have a minimum length of 2048 bits.
- The length of the modulus SHALL be divisible by 8.

EC keys SHALL be used from the following curves:

- NIST P-256
- NIST P-384

[TLS] [SMIME] Für RSA-Schlüssel gelten zusätzlich 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] Requirements from [TR2102-1] SHALL be applied.

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

6.1.6 Public key parameters generation and quality checking | Generierung und Qualitätsprüfung öffentlicher Schlüsselparameter

No stipulation.

Keine Vorgabe.

[ETSI] For RSA keys, the exponent SHALL be an odd number in the range between 2^{16} and 2^{256}.

[ETSI] Bei RSA-Schlüsseln MUSS der Exponent eine ungerade Zahl sein, die im Bereich zwischen 2^{16} und 2^{256} liegt.

[TLS] [SMIME] Keys submitted by subscribers SHALL be checked for compliance with the following characteristics:

- RSA: The value of the module SHALL be an odd number that is not the power of a prime and has no factors smaller than 752.
- ECC: The keys SHOULD be validated using either the ECC routine for full public key validation or the ECC routine for partial public key validation.

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

- 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 Key usage purposes | Schlüsselverwendung

The usage of a private key SHALL be restricted to the purposes listed in the corresponding certificate in the `keyUsage` and, if set, in the `extendedKeyUsage` (see Section 7.1.2).

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.

The usage of Root CA's private keys SHALL be limited to the signing of

- its own Root CA certificate,
- Sub CA certificates,
- OCSP Signer certificates,
- revocation lists.

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

The usage of Sub CA's private keys SHALL be limited to the signing of

- Sub CA certificates,
- subscriber certificates,
- OCSP Signer certificates,
- revocation lists and
- if applicable, OCSP responses.

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

The use of OCSP's private signing keys SHALL be limited to the signing of OCSP responses.

Die Nutzung der privaten OCSP-Signer-Schlüssel MUSS auf die Signatur von OCSP-Antworten beschränkt werden.

[QCP-n] [QCP-l] The use of the private key SHALL be restricted to the generation of electronic signatures or electronic seals.

[QCP-n] [QCP-l] Die Nutzung des privaten Schlüssels MUSS auf die Erzeugung elektronischer Signaturen bzw. elektronischer Siegel beschränkt werden.

6.2 Private Key Protection and Cryptographic Module Engineering Controls | Schutz privater Schlüssel und technische Kontrollen kryptografischer Module

To protect the private keys of all levels of the hierarchy, sufficient security measures SHALL be taken, or, in the case of subscriber keys that are not managed by the TSP, sufficient security measures SHALL be required.

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

6.2.1 Cryptographic module standards and controls | Standards und Kontrollen für kryptografische Module

Cryptographic modules used for CA- and OCSP-Signer-keys SHALL be either evaluated to CC EAL 4 or higher or to a comparable standard or certified to FIPS 140-2 level 3 or FIPS-140-3 level 3.

Die für CA- und OCSP-Signer-Schlüssel 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.

It SHALL be ensured the the devices are operated according to the specifications of the certification documentation and that it is functioning correctly.

Es MUSS sichergestellt sein, dass die Geräte gemäß den Vorgaben der Zertifizierungsdokumentation betrieben werden und korrekt funktionieren.

Manipulation of cryptographic modules during storage and transport SHALL be prevented.

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

[QCP-n-qscd] [QCP-l-qscd] QSCDs SHALL comply with the requirements set out in [eIDAS#Art.29] and be certified in accordance with [eIDAS#Art.30]. The certification status of the QSCDs SHALL be monitored until the expiration of the validity of the subscriber certificates and appropriate measures SHALL be taken if the certification status changes before expiration of the subscriber certificates.

[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] Cryptographic modules in which the keys of the Sub CAs and, if applicable, the subscribers are generated and operated SHALL be approved by the German Federal Office for Information Security for VS-NfD use.

[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 Private key (n out of m) multi-person control | Mehrpersonenkontrolle über private Schlüssel (n von m)

When importing and exporting CA keys for backup and recovery purposes (see Sections 6.2.4 and 6.2.6), a multi-person control SHALL be implemented.

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 Private key escrow | Hinterlegung privater Schlüssel

If subscriber keys are escrowed

- the keys including all copies SHALL be stored in encrypted form and protected from unauthorized access and disclosure,

Wenn Endteilnehmer-Schlüssel hinterlegt werden,

- MÜSSEN die Schlüssel inkl. aller Kopien verschlüsselt gespeichert und vor unautorisiertem Zugriff und Veröffentlichung geschützt werden,

- authentication keys and signing keys SHALL NOT be stored in a form that allows these keys to be decrypted without the control of the subscriber,
- private keys used to decrypt the stored keys SHALL NOT be used for other purposes,
- there SHALL NOT be more copies than required.

- DÜRFEN Authentisierungsschlüssel und Signaturschlüssel NICHT in einer Form hinterlegt werden, die ein Entschlüsseln dieser Schlüssel ohne Kontrolle des Zertifikatsnehmers ermöglichen,
- DÜRFEN private Schlüssel, die zur Entschlüsselung der hinterlegten Schlüssel genutzt werden, NICHT zu anderen Zwecken genutzt werden,
- DÜRFEN NICHT mehr Kopien wie erforderlich erzeugt werden.

6.2.4 Private key backup | Sicherung privater Schlüssel

Private keys of CAs and, if applicable, subscriber keys generated by the CA and intended to be backed up, SHALL be backed up in a secure environment, with the same level of security for access, tampering and loss as for the private keys in use.

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.

Backup as well as restore of CA keys SHALL be performed within the scope of a key ceremony. The same conditions apply as for the key generation (see Sections 6.1.1.1 resp. 6.1.1.2), the presence of an external auditor MAY be waived. In addition, it SHALL be ensured that access to the backups requires at least two trusted employees of the TSP.

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] If keys are backed up on behalf of subscribers
- they SHALL be stored encrypted with individual secrets generated by the Sub CA,
- the individual secrets used for encryption SHALL also be encrypted and SHALL be securely stored separately from the subscriber keys, ensuring their integrity and confidentiality,
- the subscribers SHALL be securely identified in the event of a restore application (along the lines of identification at the time of application, (see Section 4.2.1),
- the restored keys SHALL be handed over to the subscriber in the same way as the original keys (see Section 6.1.2)

[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] If keys are backed up on behalf of subscribers,
- in addition to the guidance on [3145] above, the restore actions and policies SHALL be approved by the security officer and
- other than the encryption keys SHALL NOT be backed up.

[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 Private key archival | Archivierung privater Schlüssel

No stipulation.

Keine Vorgabe.

[TLS] [SMIME] Private keys of Sub CAs SHALL NOT be archived by other parties without the permission of the TSP. Likewise, private keys of a subscriber SHALL NOT be archived without the permission of the subscriber.

[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 Private key transfer into or from a cryptographic module | Übertragung privater Schlüssel in oder von einem kryptografischen Modul

Import and export of keys SHALL be subject to a key ceremony with at least dual control. The same conditions apply as for key generation (see Sections 6.1.1.1 resp. 6.1.1.2), the presence of an external auditor MAY be waived.

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 keys SHALL NOT be exported in plain text, but the functions provided by the cryptographic module SHOULD be used to encrypt the exported keys.

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] In case of a defect of a cryptographic module used to store and use private keys of a Sub CA, the private keys SHALL be transferred to a new cryptographic module according to the requirements above.

[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 Private key storage on cryptographic module | Speicherung privater Schlüssel in kryptografischen Modulen

Keys stored in cryptographic modules SHALL be stored securely using the functions provided by the cryptographic module.

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

6.2.8 Method of activating private key | Methoden zur Aktivierung privater Schlüssel

Activation of CA private keys SHALL be performed by persons in trusted roles using the functions provided by the HSM.

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

If keys for subscribers are generated by the TSP it SHALL be ensured that the activation by the subscribers is done in a secure manner.

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] The use of private subscriber keys SHALL be in the sole control of the subscriber, regardless of whether the subscriber owns the QSCD or has it managed by a TSP on its behalf.

[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 Method of deactivating private key | Methoden zur Deaktivierung privater Schlüssel

The deactivation of CA private keys SHALL be performed by persons in trusted roles using the functions provided by the HSM.

If keys for subscribers are generated by the TSP and handed over by means of cryptographic modules (e.g., smart cards). It SHALL be ensured that their deactivation and, if necessary, reactivation by the subscribers is done in a secure manner.

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 Method of destroying private key | Methoden zur Zerstörung privater Schlüssel

Private CA keys SHALL be destroyed at the end of the life cycle of the corresponding CA certificate, i.e., upon expiration, revocation or taking out of service of the CA certificate, or termination of the Trust Service. The destruction of the keys SHALL be performed in a key ceremony and all copies of the keys SHALL be considered. The same requirements apply here as for the generation of the keys, if applicable (see Sections 6.1.1.1 resp. 6.1.1.2).

If cryptographic modules are taken out of service, all private keys stored in the module SHALL be destroyed.

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 Cryptographic Module Rating | Bewertung kryptografischer Module

Cryptographic modules SHALL be evaluated for usability and compliance with all requirements prior to purchasing.

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

6.3 Other aspects of key pair management | Andere Aspekte zur Verwaltung von Schlüsselpaaren

6.3.1 Public key archival | Archivierung des öffentlichen Schlüssels

Public keys (i.e., certificates) SHALL be retained according to Section 5.5.2.

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

6.3.2 Certificate operational periods and key pair usage periods | Nutzungsdauer von Zertifikaten und Schlüsselpaaren

The validity period of a certificate SHALL not exceed the validity period of the issuing CA certificate.

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

[ETSI] „Short-term certificates“, identified by the `id-etsi-ext-valassured-ST-certs extensions` SHALL NOT be issued.

[ETSI] „Kurzzeit-Zertifikate“, die durch die Erweiterung `id-etsi-ext-valassured-ST-certs` gekennzeichnet sind, DÜRFEN NICHT ausgestellt werden.

[QCP-n-qscd] [QCP-l-qscd] Certificates MAY be valid longer than the issuing CA certificate.

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

[TLS] [SMIME] The validity period of Root CA certificates SHALL NOT be less than 8 years and not greater than 15 years.
The validity period of Sub CA certificates SHOULD NOT be greater than 10 years.

[TLS] [SMIME] Die Gültigkeitsdauer eines Root-CA-Zertifikats DARF 8 Jahre NICHT unterschreiten und 15 Jahre NICHT überschreiten.
Die Gültigkeitsdauer eines Sub-CA-Zertifikats SOLLTE NICHT größer als 10 Jahre sein.

[TLS] Subscriber certificates SHALL NOT be valid for more than 200 days.

[TLS] Endteilnehmer-Zertifikate DÜRFEN NICHT länger als 200 Tage gültig sein.

[SMIME] Subscriber certificates SHALL NOT exceed the following validity periods: 825 days (i.e., two years plus a grace period of max. three months)

[SMIME] Endteilnehmer-Zertifikate DÜRFEN folgende Gültigkeitsdauern NICHT überschreiten: 825 Tage (d.h. zwei Jahre zzgl. einer Karenzzeit von max. drei Monaten)

[3145] The use of the private key of a Sub CA SHALL be disabled, e.g., by deactivation, if the key
- is not to be used until a defined point in time (e.g., commissioning of a new Sub CA certificate planned for the future) or
- is not to be used for a certain period of time due to a special use case.

[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 Activation data | Aktivierungsdaten

6.4.1 Activation data generation and installation | Generierung und Installation von Aktivierungsdaten

The activation data of the HSM SHALL be generated and installed during commissioning of the HSM in a four-eyes-principle within the scope of a defined change process, using the functions provided by the cryptographic module .

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.

If subscriber keys are stored in cryptographic modules (e.g., smartcards) that are provided with individual activation data (e.g., PINs), the activation data of the cryptographic modules SHALL be generated and set in a secure manner.

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 Activation data protection | Schutz der Aktivierungsdaten

Knowledge of HSM activation data SHALL be restricted to persons in trusted roles, and the group of knowing persons SHALL be strictly limited to what is absolutely necessary.

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.

If activation data for subscriber keys are generated by the TSP (see Section 6.4.1) they SHALL be protected from generation to handover to the subscriber in such a way that their integrity and confidentiality are ensured and they SHALL be handed over to the subscriber in such a way that it is time-shifted and via a different communication channel to the keys.

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 Other aspects of activation data | Andere Aspekte der Aktivierungsdaten

No stipulation.

Keine Vorgabe.

6.5 Computer security controls | Computer-Sicherheitsmaßnahmen

6.5.1 Specific computer security technical requirements | Spezifische technische Anforderungen an die Computersicherheit

Note: The requirements listed below apply by analogy to third parties contracted by the TSP, where applicable.

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

Systems required for certificate management as well as status and directory services SHALL be protected according to the potential for damage.

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

The accounts of the trusted roles (see Section 5.2.1) required to operate the critical systems SHALL be managed in such a way that

- access to the systems and data is restricted to the persons identified and authenticated for these roles (see Section 5.2.3) with the minimum required permissions,
- they are changed or deleted within a reasonable time.

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.

Remote adminsitrative access to critical systems SHALL only be allowed if it originates from systems owned or controlled by the TSP and is temporarily established over an encrypted channel based on multifactor authentication to a secured system on the TSP's network that mediates the connection to the critical systems.

Administrative 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.

For non-administrative remote access, sufficient security measures SHALL be taken to adequately protect the information accessed, processed, or stored outside the premises of the TSP

Für nicht-administrative Remote-Zugriffe MÜSSEN hinreichende Sicherheitsmaßnahmen getroffen werden, um die außerhalb der Räume des TSP abgerufenen, verarbeiteten oder gespeicherten Informationen angemessen zu schützen.

The remote access requirements SHALL be defined in a policy.

Die Vorgaben für Remote-Zugriffe MÜSSEN in einer Policy festgelegt werden.

Multi-factor authentication SHALL be implemented for the accounts that can directly initiate issuance of certificates.

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

The required separation of trusted roles (see Section 5.2.4) SHALL be technically supported by the systems.

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

Administration systems used to implement security policies SHALL NOT be used for other purposes.

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

Trusted systems that ensure the technical security and reliability of the processes supported by the systems SHALL be used.

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

The CA, certificate management, security and frontend systems and, if applicable, other internal systems supporting operation, SHALL be hardened, i.e., they SHALL be configured to disable the accounts, services, protocols and ports that are not required for operation of the CAs.

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.

If applicable, systems SHALL be equipped with integrity protection that protects against viruses, malicious code and the import of unauthorized software and is updated at least on a daily basis.

Die Systeme MÜSSEN, sofern anwendbar, mit einem Integritätsschutz versehen sein, der vor Viren, Schadcode und dem Einspielen unerlaubter Software schützt und mindestens täglich aktualisiert wird.

Systems SHALL be sized to ensure sufficient performance and uninterrupted operation.

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

Data collected for certificate generation and, if necessary, revocation, including the log data in accordance with Section 5.4.1, SHALL be protected in such a way that their integrity, confidentiality, and availability are ensured over the entire retention period.

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] Accounts of those authorized to access the system SHALL be reviewed at least every three months. Accounts that are no longer needed SHALL be deactivated.

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

Multi-factor authentication SHALL be implemented on all systems that support multi-factor authentication.

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

Authentication keys and passwords of the privileged accounts of the CA systems SHALL be changed when a person's authorization for administrative access to the systems changes or is revoked.

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.

For trusted roles, login into the systems with personal accounts for traceability SHALL be ensured.

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

For trusted roles that log in to the systems using username and password, the measures listed below SHALL be implemented, if technically possible:

- For accounts that can only be accessed in secure environments, passwords SHALL be required to be at least 12 characters in length.
- For authentications that cross a zone boundary into a secure zone, multi-factor authentication is required.
- For accounts that can be accessed from outside a secure zone, passwords of at least eight characters that are not one of the user's previous four passwords are required, and account lockout is required after five failed access attempts (see below).
- When developing password policies, TSPs SHOULD consider the password policies in NIST 800-63B Appendix A.
- If a TSP has a password policy that requires routine periodic password changes, this period SHALL NOT be less than two years.

Individuals in trusted roles SHALL be required to log out of their account or lock their workstation when they are no longer in the role.

Workstations SHALL be either configured to automatically lock out after a specified period of user inactivity, or the relevant applications SHALL be configured to automatically log out of the account after a specified period of user inactivity.

Access to CA systems SHALL be disabled after five failed login attempts, provided that the CA system supports this measure, the measure cannot be used for denial-of-service attacks, and the measure does not weaken the security of this authentication control.

Multi-factor authentication or multi-person authentication SHALL be ensured for administrative access to critical systems.

Multi-factor authentication SHALL be ensured for all accounts of trusted roles on CA systems accessible from outside the secure environments.

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 konfiguriert werden, 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.

6.5.2 Computer security rating | Sicherheitsbewertung von Computern

No stipulation.

Keine Vorgabe.

6.6 Life cycle technical controls | Technische Kontrollen des Lebenszyklus

6.6.1 System development controls | Steuerung der Systementwicklung

Already in the design and requirements specification phase of a system development project a security requirements analysis SHALL be performed to ensure that systems security is addressed from the very beginning.

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

Separate systems SHALL be used for the production, test and development environment.

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

6.6.2 Security management controls | Maßnahmen des Sicherheitsmanagements

All releases, patches and short-term bug fixes as well as configuration changes that affect the security policy, SHALL be handled and documented via regulated change management processes.

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

Any changes that impact the level of security established by the TSP, SHALL be approved by the management and if necessary, the ISMS.

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

The software used SHALL be continuously checked for newly known vulnerabilities by evaluating information from suitable sources, e.g. the "Computer Emergency Response Teams" (CERT) as well as the manufacturers. If new vulnerabilities arise in the software used, they SHALL be evaluated and, if necessary, appropriate measures must be taken to eliminate or minimize them.

Die eingesetzte Software MUSS laufend auf neu bekannt gewordene Schwachstellen durch Auswertung von Informationen aus geeigneten Quellen, z.B. der „Computer Emergency Response Teams“ (CERT) sowie der Hersteller, überprüft werden. Sofern sich bei der eingesetzten Software neue Schwachstellen ergeben, so MÜSSEN diese bewertet werden und, sofern erforderlich, geeignete Maßnahmen zur Behebung oder Minimierung getroffen werden.

It SHALL be ensured that
- security patches are applied in a reasonable amount of time, but within 6 months at the latest,
- security patches are not applied, if they introduce additional vulnerabilities or instabilities that outweigh the benefit of the patch,
- the reasons for not applying security patches are documented.

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.

The following activities SHALL be monitored continuously and appropriate alarming capabilities SHALL be implemented:
- security relevant system events according to Section 5.4.1
- availability and use of the required services
- configuration changes that were not made on the basis of an authorized change

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

The maximum interval between two integrity checks shall be documented in the CPS.

Die maximal erlaubten Intervalle der Integritätschecks der Systeme MÜSSEN in den CPS aufgeführt werden.

Monitoring SHOULD consider the sensitivity of any information collected or analyzed.

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

Backups SHOULD be tested on a regular basis to ensure that they meet the requirements of the emergency plan. The data backup and restore functions SHALL be performed by the designated trusted roles.

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] In addition to the events above, the following activities SHALL be monitored:

- changes to security profiles
- installation, update and removal of software on a certificate system
- system crashes, hardware failures, and other anomalies
- firewall and router activities
- entries into and exits out of certificate management system operating rooms

[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

System capacity needs SHALL be monitored and forecasts for future capacity needs SHALL be made to ensure adequate processing and storage capacity is available.

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 Life cycle security controls | Sicherheitsmaßnahmen während des Lebenszyklus

No stipulation.

Keine Vorgabe.

6.7 Network security controls | Netzwerk-Sicherheitsmaßnahmen

Internal networks and systems SHALL be protected from unauthorized access and attacks, e.g., by firewalls. Network components (e.g., firewalls, routers) SHALL be configured in such a way that all protocols and accesses are deactivated that are not required.

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.

Networks SHALL be segmented based on a risk assessment considering the functional, logical, and physical (including location) relationship between trustworthy systems and services.

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.

All systems critical for the operation of the TSP SHALL be located in secure or high secure zones. Root CA systems SHALL be located in high secure zones and SHALL be operated offline or separate from all other networks. Security procedures that protect the systems and communications between systems within secure zones SHALL be implemented.

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.

Local network components (e.g., routers) SHALL be installed in physically and logically secure environments. Their configurations SHALL be regularly checked for compliance with the requirements defined.

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.

Networks for administration of the systems SHALL be separated from the operational networks.

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

Within a zone, the same security requirements SHALL apply to all systems.

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

Security systems SHALL be implemented between zones to protect the systems and communications within the secure zones as well as communications with the systems outside the zones. Connections SHALL be restricted to allow only those connections required for operation. Connections not required SHALL be explicitly prohibited or disabled. All network devices at the zone boundaries (firewalls, routers, switches, gateways, or other devices) SHALL be configured to allow only those services, protocols, ports, and communication relationships that are required for the operation of the CAs.

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.

These rules SHALL be reviewed on a regular basis.

Diese Regeln MÜSSEN regelmäßig überprüft werden.

For communication between different trusted systems, trusted channels SHALL be used that are logically distinct from other communication channels and ensure secure identification of their endpoints and integrity and confidentiality of the transmitted data.

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.

If high availability of external access is required, the external network connections SHALL be redundant.

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

Vulnerability scans on public and private IP addresses identified by the TSP SHALL be performed at least quarterly. Vulnerability scans SHALL be performed by individuals or organizations with the skills, tools, abilities, ethics, and independence necessary to provide a reliable report. The execution of the vulnerability scans SHALL be documented, indicating the qualifications of the person or organization conducting the assessment.

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.

Penetration tests of the systems SHALL be performed when systems go live or when significant changes are made to the infrastructure or applications. They SHALL be performed by individuals or organizations with the skills, tools, abilities, ethics, and independence necessary to provide a reliable report. The execution of the penetration tests SHALL be documented, indicating the qualification of the person or organization performing the tests.

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.

Within 48 hours after the discovery of a critical vulnerability

- the vulnerability SHALL be remediated, or
- if remediation of the vulnerability is not possible within 48 hours, a mitigation plan for the

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

vulnerability, including prioritization based on the affected systems SHALL be prepared or
- the factual basis for the TSP's decision that the vulnerability does not need to be remediated, because either the TSP disagrees with the rating or it is not a vulnerability ("false positive") or exploitation of the vulnerability is prevented by compensating controls or the absence of threats, or other similar reasons SHALL be documented.

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] Intrusion detection (IDS) and intrusion prevention systems (IPS) that are under the control of the TSP or delegated to trusted third parties SHALL be implemented.

The vulnerability scans mentioned above SHALL be performed
- within one week upon request of the CA/Browser Forum and
- in case of significant changes to the infrastructure or applications.

[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] If an IDS is used, the log files recorded by the IDS SHALL be evaluated each time an incident occurs and periodically in a time period determined by the TSP.

[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] [ISI LANA] SHALL be used as a guide in network separation.

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

6.8 Timestamping | Zeitstempel

All systems SHALL be regularly, at least once a day, synchronized with exact time information (UTC) via a time server and the Network Time Protocol (NTP), so that the timestamps on logs and records are reliable.

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 Certifcate, CRL and OCSP Profiles | Zertifikats-, Sperrlisten- und OCSP-Profile

7.1 Certificate profiles | Zertifikatsprofile

Certificate profiles SHALL comply with [RFC5280] and [X.509] and be described in the CPSs.

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

The certificate profiles apply to all certificates issued as of the effective date of this CP. Certificates already issued with profiles in accordance with older requirements retain their validity unless explicit reference is made to their invalidity.

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.

The validity start date of a certificate SHALL NOT be before its date of issue, but it MAY be set to a later date if necessary.

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

[TLS] [SMIME] The validity period of a certificate SHALL NOT begin more than 48 hours after the time of issue.

[TLS] [SMIME] Der Gültigkeitsbeginn eines Zertifikats DARF NICHT mehr als 48 Stunden nach dessen Ausstellungszeitpunkt liegen.

Certificate serial numbers SHALL be generated using a cryptographically secure random number generator.

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

[TLS] [SMIME] Certificate serial numbers SHALL have at least 64 bits of entropy.

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

[TLS] Pre-certificates according to [RFC6962] ("Certificate Transparency") are not considered valid certificates in the sense of [RFC5280].

[TLS] Pre-Zertifikate gemäß [RFC6962] (“Certificate Transparency”) gelten nicht als gültige Zertifikate im Sinne des [RFC5280].

Note: The following lists the extensions, algorithms, and name components that are generally permitted and, where applicable, specifies requirements for their content. The certificate profiles in Appendix D specify which of the extensions and name components may or must be set in the various certificates and which may not be set.

Anmerkung: Nachfolgend werden die grundsätzlich erlaubten Erweiterungen, Algorithmen und Namensbestandteile aufgeführt und, sofern anwendbar, Vorgaben für deren Inhalte gemacht. In den Zertifikatsprofilen in Anhang D ist festgelegt, welche der Erweiterungen und Namensbestandteile in den verschiedenen Zertifikaten gesetzt werden dürfen oder müssen bzw. welche nicht gesetzt werden dürfen.

7.1.1 Version number | Versionsnummer

All X509 certificates SHALL be issued in version 3.

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

7.1.2 Certificate extensions | Zertifikatserweiterungen

Table 2 provides an overview of the certificate extensions that MAY be used. Extensions that are not listed there SHALL NOT be used, exceptions SHALL be described in the CPS.

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.

The following criticality requirements apply to the extensions listed in Table 2:

- `keyUsage` SHALL be marked as critical in all certificates.
- `basicConstraints` SHALL be marked as critical in CA certificates and MAY be marked as critical in all other certificates.
- [TLS] `basicConstraints` SHALL be marked as critical in all certificates
- [TLS] `precertificate poison extension` SHALL be marked as critical in pre certificates
- All other extensions SHALL NOT be marked as critical.

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.
- [TLS] `basicConstraints` MUSS in allen Zertifikaten als kritisch markiert werden
- [TLS] `precertificate poison extension` MUSS in allen Pre-Zertifikaten als kritisch markiert werden.
- Alle anderen Erweiterungen DÜRFEN NICHT als kritisch markiert werden.

If there are requirements for values to be set for extensions that go beyond the standard or deviate from the standard, these are listed below the table and referenced in the Requirements column. The requirements are to be interpreted in such a way that values other than the mandatory or optional values listed SHALL NOT be set.

Wenn es für Erweiterungen über den Standard hinausgehende oder vom Standard abweichende Anforderungen an die zu setzenden Werte gibt, sind diese der Tabelle nachfolgend aufgeführt und in der Spalte Anforderungen referenziert. Die Anforderungen sind so zu interpretieren, dass andere als die aufgeführten obligatorischen oder optionalen Werte NICHT gesetzt werden DÜRFEN.

Table 2 – Certficate Extensions | Tabelle 2 – Zertifikatserweiterungen

Extension | Erweiterung	OID	Requirements | Anforderungen
`authorityKeyIdentifier`	`2.5.29.35`	(01)
`subjectKeyIdentifier`	`2.5.29.14`	(01)
`keyUsage`	`2.5.29.15`	(02)-(06)
`certificatePolicies`	`2.5.29.32`	(07)-(14)
`subjectAltName`	`2.5.29.17`	(15)-(16)
`basicConstraints`	`2.5.29.19`	(17)-(18)
`extendedKeyUsage`	`2.5.29.37`	(19)-(23)
`cRLDistributionPoints`	`2.5.29.31`	(24)-(25)
`authorityInfoAccess`	`1.3.6.1.5.5.7.1.1`	(26)-(28)
`qcStatements`	`1.3.6.1.5.5.7.1.3`	(29)-(30)
`validityModel`	`1.3.6.1.4.1.8301.3.5`	-
`id-pkix-ocsp-nocheck`	`1.3.6.1.5.5.7.48.1.5`	see Section 7.3 | siehe Kap. 7.3
`cabfOrganizationIdentifier`	`2.23.140.3.1`	(31)
`signedCertificateTimestampList`	`1.3.6.1.4.1.11129.2.4.2`	(32)
`precertificate poison extension`	`1.3.6.1.4.1.11129.2.4.3`	(33)

`authorityKeyIdentifier, subjectKeyIdentifier`

(01) The `keyIdentifier` SHALL be set according to [RFC5280#4.2.1.1] and SHALL match the `subjectKeyIdentifier` of the issuing CA.

Es MUSS der `keyIdentifier` gemäß [RFC5280#4.2.1.1] gesetzt werden, dieser MUSS dem `subjectKeyIdentifier` der ausstellenden CA entsprechen.

`keyUsage`

(02) In CA certificates, `keyCertSign` SHALL be set. If the CA also signs revocation lists, `cRLSign` SHALL be set additionally.

In CA-Zertifikaten MUSS `keyCertSign` gesetzt sein. Sofern die CA auch Sperrlisten signiert, MUSS zusätzlich `cRLSign` gesetzt werden.

(03) In OCSP-Signer certificates `digitalSignature` SHALL be set.

In OCSP-Signer-Zertifikaten MUSS `digitalSignature` gesetzt werden.

(04) [ETSI] In subscriber certificates for natural persons or organizations, one of the following variants of the `keyUsage` SHALL be set:
a) `nonrepudiation`
b) `nonRepudiation` and `digitalSignature`
c) `digitalSignature`
d) `digitalSignature` and [`keyEncipherment` or `keyAgreement`]
e) `keyEncipherment` or `keyAgreement`
f) `nonrepudiation` and `digitalSignature` and [`keyEncipherment` or `keyAgreement`]

To avoid mixed use of keys, only variants a), c) or e) SHOULD be used.

[QCP-n] [QCP-l] One of the variants a), b) or f) SHALL be used, of which variant a) SHOULD be used.

[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.

[QCP-n] [QCP-l] Es MUSS eine der Varianten a), b) oder f) genutzt werden, davon SOLLTE Variante a) genutzt werden.

(05) [SMIME] In subscriber certificates `keyUsage` SHALL be set according to the application purpose one of the variants b), c), d), e) or f) listed under (05).

[SMIME] In Endteilnehmer-Zertifikaten MUSS die `keyUsage` gemäß dem Anwendungszweck eine der unter (04) aufgeführten Varianten b), c), d), e) oder f) gesetzt werden.

(06) [TLS] In subscriber certificates `keyUsage` SHALL be set according to the application purpose one of the variants c) or d) listed under (05), of which variant c) SHOULD be set.

[TLS] In Endteilnehmer-Zertifikaten MUSS die `keyUsage` gemäß dem Anwendungszweck eine der unter (04) aufgeführten Varianten c) oder d) gesetzt werden, davon SOLLTE Variante c) genutzt werden.

`certificatePolicies`

(07) In principle, only OIDs SHOULD be set in the certificatePolicies. If the sole use of OIDs is insufficient, `cPSuri` with a valid http- or https-URL MAY be set additionally.

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 gesetzt werden.

(08) [TLS] In Sub-CA certificates, either `anyPolicy` or the applicable OID according to [BR] SHALL be set.
If the [BR] applicable OID is set, the following requirements apply:
- More than one OID as specified in [BR] SHALL NOT be set.
- In addition, however, further OIDs according to [ETSI] MAY be set.

[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] gesetzt werden.

(09) [SMIME] In Sub-CA certificates, either `anyPolicy` or the applicable OID(s) according to [SBR] SHALL be set. If the [SBR] applicable OID(s) are set, further OIDs according to [ETSI] as well as OIDs of the TSP described in the relevant CPS MAY be set.

[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.

(10) [TLS] [SMIME] The `certificatePolicies` set in Sub CA and subscriber certificates SHALL correspond

[TLS] [SMIME] Die in Sub-CA- und Endteilnehmer-Zertifikaten gesetzten `certificatePolicies` MÜSSEN

	to each other, i.e., subscriber certificates SHOULD NOT be issued by a Sub CA with OIDs that are not contained in the Sub CA certificate itself, unless `anyPolicy` is set in the Sub CA certificate ("policy chaining").	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“).
(11)	[ETSI] Subscriber certificates for natural or legal persons (not SSL server certificates) SHALL include at least one OID that reflects the practices and procedures performed by the TSP. [LCP] [NCP] The applicable OID reserved by ETSI MAY be set: ▪ NCP: `0.4.0.2042.1.1` ▪ LCP: `0.4.0.2042.1.3` [QCP] The applicable OID reserved by ETSI SHALL be set: ▪ 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`	[ETSI] In Endteilnehmer-Zertifikaten für natürliche Personen oder Organisationen MUSS mindestens eine OID gesetzt sein. [LCP] [NCP] Die jeweils anwendbare von ETSI reservierte OID DARF gesetzt werden: ▪ NCP: `0.4.0.2042.1.1` ▪ LCP: `0.4.0.2042.1.3` [QCP] Die jeweils anwendbare von ETSI reservierte OID MUSS gesetzt werden: ▪ 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`
(12)	[TLS] Subscriber certificates SHALL contain the corresponding OID according to [BR]: ▪ EVCP: `2.23.140.1.1` ▪ DVCP: `2.23.140.1.2.1` ▪ OVCP: `2.23.140.1.2.2` [QCP] The corresponding ETSI OID SHALL also be included: ▪ QEVCP-w: `0.4.0.194112.1.4` ▪ QNCP-w: `0.4.0.194112.1.5` In addition, the subsequent ETSI reserved OIDs MAY be used: ▪ EVCP: `0.4.0.2042.1.4` ▪ DVCP: `0.4.0.2042.1.6` ▪ OVCP: `0.4.0.2042.1.7`	[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` [QCP] Es MUSS 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 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`
(13)	[EVCP] In subscriber certificates, `cPSuri` SHALL be set with a reference (http URL) to the CPS.	[EVCP] In Endteilnehmer-Zertifikaten MUSS `cPSuri` mit einem Verweis (http URL) zum CPS gesetzt werden.
(14)	[SMIME] In subscriber certificates, at least the corresponding [SBR] OID for the Multipurpose Generation SHALL be set: ▪ Mail Validated: `2.23.140.1.5.1.2` ▪ Organization Validated: `2.23.140.1.5.2.2` ▪ Sponsor Validated: `2.23.140.1.5.3.2` ▪ Individual Validated: `2.23.140.1.5.4.2` In addition, the TSP's own OIDs, which are described in the relevant CPS and/or the ETSI reserved OIDs (see (13)) MAY be used.	[SMIME] In Endteilnehmer-Zertifikaten MUSS mindestens die korrespondierende OID der Multipurpose-Generation gemäß [SBR] gesetzt sein: ▪ Mail Validated: `2.23.140.1.5.1.2` ▪ Organization Validated: `2.23.140.1.5.2.2` ▪ Sponsor Validated: `2.23.140.1.5.3.2` ▪ Individual Validated: `2.23.140.1.5.4.2` 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.

subjectAltName

(15)	[TLS] In subscriber certificates, at least one entry SHALL be included in the `subjectAltName`. Permitted entries are FQDNs or Wildcard Domain Names as `dNSName` or IPv4 or IPv6 addresses as `iPAddress`. The FQDNs as well as the FQDN portions of Wildcard Domain Names SHALL consist exclusively of "P-Labels" or "Non-Reserved LDH-Labels". Reserved IP addresses or internal names (according to Annex C) SHALL NOT be included.	[TLS] 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.
(16)	[SMIME] In subscriber certificates, at least one email address as `rFC822Name` SHALL be included in the `subjectAltName`.	[SMIME] In Endteilnehmer-Zertifikaten MUSS mindestens eine E-Mail-Adresse als `rFC822Name` im `subjectAltName` aufgenommen werden.

basicConstraints

(17)	In CA certificates, `cA` SHALL be set to true. In Sub CA certificates a maximum path length SHOULD be indicated in `pathLenConstraints`, In Root CA certificates this indication SHOULD NOT be made.	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.
(18)	In subscriber and OCSP-Signer certificates, `cA` SHALL be set to `false`. `pathLenConstraints` SHALL NOT be set.	In Endteilnehmer- und OCSP-Signer-Zertifikaten MUSS `cA` auf `false` gesetzt sein, `pathLenConstraint` DARF NICHT gesetzt werden.

extendedKeyUsage

(19)	If the `extendedKeyUsage` is set, it SHALL be set consistently with the keyUsage according to [RFC5280#4.2.1.12].	Wenn die `extendedKeyUsage` gesetzt ist, MUSS diese gemäß [RFC5280#4.2.1.12] konsistent zur keyUsage sein.
(20)	[TLS] In subscriber and Sub CA certificates[9] , `id-kp-serverAuth` SHALL be set. In addition, `id-kp-clientAuth` MAY be set.	[TLS] In Enteilnehmer- und Sub-CA-Zertifikaten[10] MUSS `id-kp-serverAuth` eingetragen werden. Es DARF darüber hinaus `id-kp-clientAuth` eingetragen werden.
(21)	[SMIME] In susbcriber and Sub CA certificates[9] , `id-kp-emailProtection` SHALL be set. In addition, `id-kp-clientAuth` MAY be set.	[SMIME] In Endteilnehmer- und Sub-CA-Zertifikaten[10] MUSS `id-kp-emailProtection` eingetragen werden. Es DARF darüber hinaus `id-kp-clientAuth` eingetragen werden.
(22)	[TLS] [SMIME] The `extendedKeyUsage` set in Sub CA and subscriber certificates SHALL correspond to each other, i.e., subscriber certificates SHALL NOT be issued by a Sub CA with values that are not contained in the Sub CA certificate itself ("EKU chaining").	[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“).

[9] This requirement does not apply to cross certificates ; see the specifications in [BR], [SBR], and [CCADB] for more information.
[10] Diese Anforderung gilt nicht für Cross-Zertifikate, siehe hierzu die Festlegungen in [BR], [SBR] und [CCADB].

	This does not apply to OCSP Signer certificates, which MAY also be issued by Sub CAs that do not contain `id-kp-OCSPSigning`.	Hiervon ausgenommen sind OCSP-Signer-Zertifikate, die auch von Sub-CAs ausgestellt werden DÜRFEN, welche selbst nicht `id-kp-OCSPSigning` enthalten.
(23)	In OCSP Signer certificates, `id-kp-OCSPSigning` SHALL be set.	In OCSP-Signer-Zertifikaten MUSS `id-kp-OCSPSigning` eingetragen werden.

`cRLDistributionPoints`

(24)	[TLS] [SMIME] In Sub CA and subscriber certificates, `cRLDistributionPoints` SHALL be set with at least one http URL in `distributionPoints`. `Reasons` and `CRLIssuer` SHALL NOT be set.	[TLS] [SMIME] In Sub-CA- und Endteilnehmer-Zertifikaten MÜSSEN `cRLDistributionPoints` mindestens eine http-URL in `distributionPoints` enthalten. `Reasons` und `CRLIssuer` DÜRFEN NICHT gesetzt werden
(25)	[3145] [ETSI] In subscriber certificates, the `cRLDistributionPoints` extension SHALL be set with at least one publicly accessible http or ldap URL in `distributionPoints`.	[3145] [ETSI] In Endteilnehmer-Zertifikaten MÜSSEN `cRLDistributionPoints` mindestens eine öffentlich erreichbare http- oder ldap-URL in `distributionPoints` enthalten.

`authorityInfoAccess`

(26)	`authorityInfoAccess` SHALL contain at least the http URL of the OCSP responder in `id-ad-ocsp`.	`authorityInfoAccess` MUSS mindestens die http-URL des OCSP-Responders in `id-ad-ocsp` enthalten.
(27)	[TLS] [SMIME] In Sub CA certificates, the http URL to download the issuing CA certificate SHOULD also be included in `caIssuers`.	[TLS] [SMIME] In Sub-CA- Zertifikaten SOLLTE zusätzlich die http-URL zum Abruf des ausstellenden CA-Zertifikats in `caIssuers` enthalten sein.
(28)	[ETSI] In subscriber certificates, the http URL to download the issuing CA certificate SHALL also be included in `caIssuers`.	[ETSI] In Endteilnehmer-Zertifikaten MUSS mindestens eine http(s)-URL zum Abruf des ausstellenden CA-Zertifikats in `caIssuers` enthalten sein.

`qcStatements`

(29)	[QCP] In subscriber certificates, the following qcStatements SHALL be set :
	▪ `qcs-QcCompliance`: `0.4.0.1862.1.1`
	▪ `qcs-QcPDS`: `0.4.0.1862.1.5`
	▪ `qcs-QcType`[11]: `0.4.0.1862.1.6` with one of the following values:
	  ▪ `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`
	
	In addition, the following qcStatements MAY be set:
	▪ `qcs-QcLimitValue`: `0.4.0.1862.1.2`
		[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`[12]: `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:

[11] Cerficates for QES: optional
[12] Zerfikate für QES: optional

	▪ qcs-QcRetentionPeriod: 0.4.0.1862.1.3 qcs-qcCClegislation(0.4.0.1862.1.7) SHALL NOT be set. Regarding the syntax of the qcStatements, [ETS4125] SHALL be considered.	▪ 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.
(30)	[QCP-n-qscd] [QCP-l-qscd] In subscriber certificates, qcs-QcSSCD(0.4.0.1862.1.4) SHALL be set.	[QCP-n-qscd] [QCP-l-qscd] In Endteilnehmer-Zertifikaten MUSS qcs-QcSSCD (0.4.0.1862.1.4) gesetzt werden.

cabfOrganizationIdentifier

(31)	[EVCP] The cabfOrganizationIdentifier SHALL reference the same registration as the organizationIdentifier.	[EVCP] Der cabfOrganizationIdentifier MUSS die gleiche Registrierung referenzieren wie der organizationIdentifier.

signedCertificateTimestampList

(32)	[TLS] In subscriber certificates, at least three SCTs from two different CTLog operators SHALL be included.	[TLS] In Endteilnehmer-Zertifikaten MÜSSEN mindestens drei SCT von zwei unterschiedlichen CTLog-Betreibern enthalten sein.

precertificate poison extension

(33)	[TLS] In pre-certificates the precertificate poison extension SHALL be set according to [RFC6962].	[TLS] In Pre-Zertifikaten MUSS die Erweiterung precertificate poison extension gemäß [RFC6962] gesetzt werden.

7.1.3 Algorithm object identifiers | Algorithmen-OID

Algorithms used for signing certificates SHOULD comply with the requirements from [SOGIS].

CA certificates, that are based on an RSA key, SHALL use one of the following signature algorithms to sign the certificates they issue:

- sha256WithRSAEncryption (1.2.840.113549.1.1.11)
- sha384WithRSAEncryption (1.2.840.113549.1.1.12)
- sha512WithRSAEncryption (1.2.840.113549.1.1.13)
- rsassa-pss(1.2.840.113549.1.1.10)
  - MGF-1 with SHA-256, and a salt length of 32 bytes
  - MGF-1 with SHA-384, and a salt length of 48 bytes
  - MGF-1 with SHA-512, and a salt length of 64 bytes

Die für die Signatur der Zertifikate aller Hierarchieebenen verwendeten Algorithmen SOLLTEN 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)
- sha384WithRSAEncryption (1.2.840.113549.1.1.12)
- sha512WithRSAEncryption (1.2.840.113549.1.1.13)
- rsassa-pss(1.2.840.113549.1.1.10)
  - MGF-1 with SHA-256, and a salt length of 32 bytes
  - MGF-1 with SHA-384, and a salt length of 48 bytes
  - MGF-1 with SHA-512, and a salt length of 64 bytes

CA certificates based on a P256 ECDSA key SHALL use `ecdsa-with-SHA256(1.2.840.10045.4.3.2)` to sign the certificates they issue.

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.

CA certificates based on a P384 ECDSA key SHALL use `ecdsa-with-SHA384(1.2.840.10045.4.3.3)` to sign the certificates they issue.

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.

CA certificates based on a P521 ECDSA key SHALL use `ecdsa-with-SHA512(1.2.840.10045.4.3.4)` to sign the certificates they issue.

CA-Zertifikate, die auf einem P521-ECDSA-Schlüssel basieren, MÜSSEN zur Signatur der von ihnen ausgestellten Zertifikate den Signaturalgorithmus `ecdsa-with-SHA512 (1.2.840.10045.4.3.4)` verwenden.

For certificates based on RSA keys, `rsaEncryption (1.2.840.113549.1.1.1)` SHALL be set with `NULL` parameter in the subjectPublicKeyInfo.

Zertifikate, die auf RSA-Schlüsseln basieren, MÜSSEN `rsaEncryption (1.2.840.113549.1.1.1)` mit `NULL` Parameter in der subjectPublicKeyInfo enthalten.

For certificates based on ECDSA keys, `ecPublicKey (1.2.840.10045.2.1)` SHALL be set without `NULL` parameter and depending on the used curve of one of the following OIDs of the subjectPublicKeyInfo:

- P256: `prime256v1(1.2.840.10045.3.1.7)`
- P384: `secp384r1(1.3.132.0.34)`
- P521: `secp521r1(1.3.132.0.35)`

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)`
- P384: `secp384r1(1.3.132.0.34)`
- P521: `secp521r1(1.3.132.0.35)`

Algorithms and parameters used SHALL be listed in the CPSs.

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

Note: Regarding the encoding, please refer to [BR#7.1.3].

Hinweis: Bzgl. der Codierung sei auf [BR#7.1.3] verwiesen.

7.1.4 Name forms | Namensformen

General regulations:

- The `issuerDN` of a certificate SHALL correspond to the `subjectDN` of the issuing certificate "byte-by-byte".
- `subjectDN` attributes SHALL NOT be set more than once.
- [TLS] In subscriber certificates the attributes SHALL be encoded and set in the order according to [BR#7.1.4.2].

Grundsätzliches:

- Der `issuerDN` eines Zertifikats MUSS dem `subjectDN` des ausstellenden Zertifikats „Byte-für-Byte“ entsprechen.
- Die Attribute des `subjectDN` DÜRFEN NICHT mehr als einmal gesetzt werden.
- [TLS] In Endteilnehmer-Zertifikaten MÜSSEN die Attribute gemäß [BR#7.1.4.2] codiert und in der dort aufgeführten Reihenfolge gesetzt werden.

Table 3 provides an overview of usable `subjectDN` attributes for CA, subscriber and OCSP Signer certificates. Attributes, that are not listed there SHALL NOT be set in principle, exceptions SHALL be described in the CPS.

Tabelle 3 gibt einen Überblick über die nutzbaren 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.

If there are requirements for attributes that go beyond the standard or deviate from the standard in terms of the content to be set, these are listed below the table and referenced in the Requirements column. The requirements are

Wenn es für Attribute über den Standard hinausgehende oder vom Standard abweichende Anforderungen an die zu setzenden Inhalte gibt, so sind diese der Tabelle nachfolgend aufgeführt und in der Spalte Anforderungen referenziert. Die Anforderungen sind

to be interpreted in such a way that values other than the mandatory or optional values listed SHALL NOT be set.

so zu interpretieren, dass andere als die aufgeführten obligatorischen oder optionalen Werte NICHT gesetzt werden DÜRFEN.

Table 3 – Name forms | Tabelle 3 – Namensformen

subjectDN attribute | Attribut	OID	Requirements | Anforderungen
commonName	2.5.4.3	(01)-(04)
emailAddress	1.2.840.113549.1.9.1	(05)
title	2.5.4.12	-
serialNumber	2.5.4.5	(06)-(08)
givenName	2.5.4.42	see Section 3.1.2 | siehe Kap. 3.1.2
surname	2.5.4.4	see Section 3.1.2 | siehe Kap. 3.1.2
pseudonym	2.5.4.65	-
streetAddress	2.5.4.9	(09)
localityName	2.5.4.7	(09)
stateOrProvinceName	2.5.4.8	(09)
postalCode	2.5.4.17	(09)
businessCategory	2.5.4.15	(10)
organizationalUnitName	2.5.4.11	-
organizationIdentifier	2.5.4.97	(11)-(12), see Section 3.1.2 | siehe Kap. 3.1.2
jurisdiction.LocalityName	1.3.6.1.4.1.311.60.2.1.1	see Annex D4.1 | siehe Anhang D 4.1
jurisdiction.StateOrProv.Name	1.3.6.1.4.1.311.60.2.1.2	see Annex D4.1 | siehe Anhang D 4.1
jurisdiction.CountryName	1.3.6.1.4.1.311.60.2.1.3	see Annex D4.1 | siehe Anhang D 4.1
organizationName	2.5.4.10	see Section 3.1.2 | siehe Kap. 3.1.2
countryName	2.5.4.6	(13)-(14)

commonName

(01) In CA certificates, the commonName SHALL be unique across all certificates generated by the issuing CAand SHALL include a common name (i.e., not necessarily the full registered name) of the TSP.

In CA-Zertifikaten MUSS der commonName über alle von der ausstellenden CA erzeugten Zertifikate hinweg eindeutig sein und den Namen (nicht unbedingt der vollständige registrierte Name) des TSP beinhalten.

(02) In Root CA certificates the commonName SHALL NOT be reused, i.e., in subsequent certificates another commonName SHALL be assigned.

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

(03) [TLS] The commonName in subscriber certificates SHALL contain exactly one entry that is also contained in the subjectAltName. Regarding the encoding of the commonName applies:

- IPv4 addresses SHALL be encoded according to [RFC3986],
- IPv6 addresses SHALL be encoded according to [RFC5952#4],
- FQDN and wildcard domain names SHALL be a character-by-character copy of the corresponding dNSName entry from the subjectAltName .

[TLS] In Endteilnehmer-Zertifikaten MUSS der commonName 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] The commonName in subscriber certificates MAY be set with the mailbox address as specified in the subjectAltName.

[SMIME] In Endteilnehmer-Zertifikaten DARF der commonName eine Mailbox-Adresse, wie im subjectAltName angegeben, enthalten.

In Organization Validated Certificates the organization name MAY alterantively be set as specified in `organization`. In Individual or Sponoser validated the name of the person or the `pseudonym` MAY alterantively be set.	In Orgnaisations-validierten Zertifikaten DARF alternativ der Name der Organisation wie in `organization` angegeben gesetzt werden. In Individual- oder Sponosr-validierten Zertifikaten DARF alternativ der Name der Person oder das `pseudonym` gesetzt werden.

`emailAddress`

(05)	[SMIME] The `emailAddress` in subscriber certificates SHALL contain a value, that is also set in the `subjectAltName`.	[SMIME] In Endteilnehmer-Zertifikaten MUSS `emailAddress` mit einer Mailbox-Adresse, wie im `subjectAltName` angegeben, gesetzt werden.

`serialNumber`

(06)	[ETSI] The `serialNumber` SHALL ensure the uniqueness of the name, it has no defined semantics.	[ETSI] Die `serialNumber` MUSS die Eindeutigkeit des Namens gewährleisten, sie hat keine definierte Semantik.
(07)	[SMIME] The `serialNumber` in subscriber certificates SHALL be set with an identifier assigned by the CA or RA to identify or distinguish the subscriber.	[SMIME] Die `serialNumber` MUSS mit einem von der CA oder RA vergebenen Identifier zur Identifizierung oder Unterschei-dung des Zertifikatsnehmers gesetzt werden.
(08)	[EVCP] In subscriber certificates, the `serialNumber` SHALL contain the legally assigned number (incorporation number or similar number) of the organization. If no such number has been assigned, the date of incorporation SHALL be set in a common date format. For Government Entities that cannot provide a registration number or date of incorporation, an appropriate description SHALL be included to indicate that the organization is a Government Entity.	[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, die keine Registrierungsnummer oder Gründungsdatum nachweisen können, MUSS eine geeignete Beschreibung aufgenommen werden, um anzuzeigen, dass es sich bei der Organisation um eine Behörde handelt.

`streetAddress, postalCode, localityName, stateOrProvinceName`

(09)	[TLS] [SMIME] If the `streetAddress`, `postalCode`, `localityName` or `stateOrProvinceName` are set in subscriber certificates, they SHALL contain the physical address of the place of business of the subscriber.	[TLS] [SMIME] Wenn in Endteilnehmer-Zertifikaten `streetAddress`, `postalCode`, `localityName` und/oder `stateOrProvinceName` gesetzt werden, MÜSSEN diese die Adresse des Geschäftssitzes des Zertifikatsnehmers enthalten.

`businessCategory`

(10)	[EVCP] `businessCategory` SHALL be set with the applicable organization type according to Section 1.3.3.	[EVCP] `businessCategory` MUSS mit dem korrekten Organisationstyp gemäß Kap. 1.3.3 gesetzt warden.

organizationIdentifier

(11) [ETSI] If the `organizationIdentifier` is set, it SHALL contain a registration number, if any, of the organization according to the following scheme:
- three characters for the registration scheme (`VAT`, `LEI` or `NTR`)
- two characters for the country code
- a hyphen ("-")
- reference assigned according to the identified registration scheme

For Government Entities that do not have one of the above registration numbers, `GOV` SHALL be used as the registration scheme as follows:
- `GOV` for the registration scheme
- country code
  - federal authority: two characters ISO 3166-1 country code, e.g., `GOVDE`
  - state/province-level authority: two characters of ISO 3166-1 country code, the plus sign ("+") and up to 3 characters of ISO 3166-2 code for the state/province, e.g., `GOVDE+NW`

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

Für Behörden, die über keine der o.g. Registrierungsnummern verfügen, MUSS als Registrierungsschema GOV wie folgt verwendet werden:
- `GOV` für das Registrierungsschema
- Ländercode
  - Behörden auf Bundesebene: zwei Zeichen ISO 3166-1 Ländercode, z.B. `GOVDE`
  - Behörde auf Landesebene: zwei Zeichen ISO 3166-1 Ländercode, das Plus-Zeichen („+“) und bis zu 3 Zeichen ISO 3166-2 Code für das Bundesland, z.B. `GOVDE+NW`

(12) [EVCP] `LEI` SHALL NOT be set as registration scheme.

[EVCP] `LEI` DARF NICHT als Registrierungsschema verwendet werden

countryName

(13) If the `countryName` is set, it SHALL contain the two-character country code of the subscriber according to ISO 3166-1.

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

(14) [ETSI] If the `pseudonym` is set, `countryName` SHOULD be set with the value "`DE`" (country of CA's location). For certificates for natural persons in association with an organization, the country of the organization's location MAY alternatively be set as the `countryName`.

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

7.1.5 Name constraints

`nameConstraints` SHALL NOT be set.

`nameConstraints` DÜRFEN NICHT gesetzt werden.

7.1.6 `certificatePolicies` object identifier | OIDs der Erweiterung `certificatePolicies`

See Section 7.1.2.

Siehe Kap. 7.1.2.

7.1.7 Usage of `policyConstraints` extension | Verwendung der Erweiterung `policyConstraints`

`policyConstraints` SHALL NOT be set.

`policyConstraints` DÜRFEN NICHT gesetzt werden.

7.1.8 `policyQualifiers` syntax and semantics | Syntax und Semantik der `policyQualifier`

`policyQualifiers` SHALL be set conforming to [RFC5280] with the contents defined in Section 7.1.2.

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

7.1.9 Processing semantics for `certificatePolicies` | Verarbeitungssemantik für `certificatePolicies`

`certificatePolicies` SHALL NOT be marked as critical, so it is up to the decision of the certificate users to evaluate this extension.

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

7.2 CRL profile | Sperrlistenprofile

All revocation lists SHALL comply with the requirements of [RFC5280].

Alle Sperrlisten MÜSSEN den Anforderungen des [RFC5280] genügen.

The algorithms listed in Section 7.1.3 SHALL be used for signing the revocation lists.

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

All CRLs SHALL be direct and full CRLs, i.e. they SHALL be issued from the CA and SHALL contain at least all revoked and still valid certificates issued from this CA. In addition, the CRLs MAY contain also the revoked and expired certificates issued from this CA.

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 Version number | Versionsnummer

All revocation lists SHALL be issued in X.509 version 2.

Alle Sperrlisten MÜSSEN in X.509 Version 2 ausgestellt werden.

7.2.2 CRL and CRL entry extensions

All revocation lists SHALL contain at least the `authorityKeyIdentifier` and `cRLNumber` CRL extensions.

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

CARLs SHALL contain the CRL entry extension `reasonCode`, CRLs MAY contain it.

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

If expired certificates are not removed from the revocation list, the revocation list SHALL contain the `expiredCertsOnCRL` extension. If expired certificates are removed from the revocation list, the revocation list SHALL NOT contain `expiredCertsOnCRL`.

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 SHALL contain the CRL entry extension `reasonCode`, if any of the following revocation reasons exist (see also Section 4.9.1.2):

- `keyCompromise`
- `privilegeWithdrawn`
- `cessationOfOperation`
- `affiliationChanged`
- `superseded`
- [SMIME] `certificateHold`

If the revocation reason does not match any of the above-mentioned revocation reasons, the `reasonCode` SHALL NOT be set.

[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`
- [SMIME] `certificateHold`

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

All extensions SHALL NOT be marked as critical.

Alle Erweiterungen DÜRFEN NICHT als kritisch markiert werden.

7.3 OCSP Profile | OCSP-Profil

All OCSP responses SHALL meet the requirements of [RFC6960] and SHALL be signed either by the CA itself or by an OCSP Signer whose certificate has been issued by the CA.

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.

If the OCSP responses are signed by a dedicated OCSP Signer, `id-pkix-ocsp-nocheck` SHALL be set in the OCSP signer certificate and contain the value NULL. `cRLDistributionPoints` and `authorityInfoAccess` SHALL NOT be set, and the OCSP signer certificate SHOULD have a short validity period and be renewed regularly due to the inability to check its status.

Wenn die OCSP-Antworten durch einen eigens dafür vorgesehenen OCSP-Signer signiert werden, so MUSS `id-pkix-ocsp-nocheck` im OCSP-Signer-Zertifikat gesetzt werden und den Wert NULL enthalten. `cRLDistributionPoints` und `authorityInfoAccess` DÜRFEN NICHT gesetzt werden und das OCSP-Signer-Zertifikat SOLLTE aufgrund der fehlenden Prüfmöglichkeit seines Status eine kurze Gültigkeitsdauer haben und regelmäßig erneuert werden.

The algorithms listed in Section 7.1.3 SHALL be used for signing the OCSP responses.

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

[TLS] [SMIME] OCSP responses for revoked Sub-CA or cross-certificates SHALL contain the revocation reason in the `revocationReason` attribute within the `revokedInfo` (not in the extensions, see Section 7.3.2). The specifications made in Section 7.2.2 apply with regard to the revocation reasons.

[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 Version number | Versionsnummer

OCSP in version 1 according to [RFC6960] SHALL be used.

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

7.3.2 OCSP extensions | OCSP Erweiterungen

No stipulation.

Keine Vorgabe.

[TLS] [SMIME] The `reasonCode` extension according to [RFC5280#5.3.1] SHALL NOT be set in OCSP responses (see also Section 7.3).

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

[QCP] The `archiveCutOff` extension SHOULD be set in the response with the time of the validity start of the referenced CA certificate.

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

8 Compliance audit and other assessments | Audits und andere Bewertungskriterien

8.1 Frequency or circumstances of assessment | Häufigkeit und Art der Prüfungen

8.1.1 Internal audits | Selbstüberprüfung

No stipulation.	Keine Vorgabe.
[TLS] [SMIME] Compliance with the requirements of this CP and the applicable CPS, as well as their quality of service, SHALL be monitored through appropriate internal audits during the period in which subscriber certificates are issued. These internal audits SHALL be conducted at least quarterly and SHALL include random sampling of at least three percent of the subscriber certificates ([SMIME] at least 30 certificates) issued since the last internal audit.	[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 ([SMIME] mindestens 30 Zertifikate) umfassen, die seit der letzten Selbstüberprüfung ausgestellt wurden.

8.1.2 External Audits | Prüfungen durch externe Auditoren

No stipulation.	Keine Vorgabe.
[TLS] [SMIME] Trust Services SHALL be audited in a continuous sequence of audit periods from the generation of a CA key pair to its destruction and withdrawal of trust ("cradle-to-grave") according to an audit scheme listed in Section 8.4 ("period-of-time audits"), whereby a period SHALL NOT exceed the duration of one year	[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] Trust Services SHALL be audited annually according to Section 8.4.	[3145] Die Trust Services MÜSSEN jährlich gemäß Kap. 8.4 geprüft werden.
[QCP] Trust Services SHALL be audited by a Conformity Assessment Body at least every 24 months.	[QCP] Die Trust Services MÜSSEN mindestens alle 24 Monate von einer Konformitätsbewertungsstelle geprüft werden.

8.1.3 Audits of subcontractors and delegated third parties | Prüfungen von Unterauftragnehmern und delegierten Dritten

No stipulation.	Keine Vorgabe.
[TLS] [SMIME] The practices and procedures of all delegated third parties SHALL be reviewed at least annually for compliance with the requirements of this CP and the applicable CPS.	[TLS] [SMIME] Es MÜSSEN die Praktiken und Verfahren aller delegierten Dritten mindestens jährlich bzgl. der Einhaltung der Anforderungen dieser CP und der anwendbaren CPS überprüft werden.
[3145] Subcontractors or delegated third parties SHALL be audited in the applicable areas to the same extent in accordance with the requirements of [3145] as the	[3145] Unterauftragnehmer oder delegierte Dritte MÜSSEN in den anwendbaren Bereichen in demselben Umfang gemäß den Anforderungen aus [3145] geprüft werden, wie der Betrieb der TSP

operation of the TSP itself. This requirement SHALL be contractually agreed with the subcontractors or delegated third parties.

selbst. Diese Anforderung MUSS vertraglich mit den Unterauftragnehmern oder delegierten Dritten vereinbart werden.

8.2 Identity/qualifications of assessor | Identität/Qualifikation der Prüfer

Internal auditors performing the internal audits according to Section 8.1.1 and the audits of subcontractors and delegated third parties according to Section 8.1.3 SHALL have sufficient experience as auditors and expertise in PKI technologies and processes.

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.

External auditors performing audits in accordance with Section 8.1.2 SHALL be qualified auditors who have the following qualifications and skills, i.e., they SHALL

- be independent from the subject of the audit,
- be able to conduct audits that addresses the criteria specified in eligible audit schemes according to Section 8.4,
- employ individuals who have proficiency in examining PKI technologies, information security tools and techniques, information technology and security auditing and the third-party attestation function,
- be bound by law, government regulations, or professional code of ethics.

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.

For auditing according to the ETSI standards, the evaluation body SHALL also be accredited by "DAkkS" (German Accreditation Body) according to ISO 17065 using the requirements defined in ETSI EN 319 403 and SHALL be a member of the „Accredited Conformity Assessment Bodies' Council" (ACAB'c).

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] External auditors SHALL maintain a professional liability errors and omissions insurance with coverage of at least one million dollars.

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

[QCP] The Trust Services SHALL be audited by Conformity Assessment Bodies meeting the requirements of ETSI EN 319 403.

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

[3145] Audits SHALL be performed by ISO 27001 auditors.

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

8.3 Assessor's relationship to assessed entity | Beziehung des Prüfers zur geprüften Stelle

External auditors performing the audits according to Section 8.1.2 SHALL be independent of the audited entity and item.

For internal auditors, the separation of roles according to Section 5.2.4 SHALL be observed.

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 Topics covered by assessment | Abgedeckte Bereiche der Prüfung

No stipulation.

Keine Vorgabe.

[TLS] [SMIME] The Trust Services SHALL be audited according to ETSI EN 319 411-1 or ETSI 319 411-2 or ETSI TS 119 411-6 in an applicable version whereby the respective current version SHOULD be used.

[TLS] [SMIME] Die Trust Services MÜSSEN nach ETSI EN 319 411-1 oder -2 bzw. ETSI TS 119 411-6 in einer anwendbaren Version geprüft werden, dabei SOLLTE die jeweils aktuelle Version zugrunde gelegt werden.

[TLS] Applicable policies are DVCP, OVCP or QNCP-w.

[TLS] Anwendbare Policies sind DVCP, OVCP oder QNCP-w.

[SMIME] Applicable policies are:
- LCP or Mail, Organization, or Sponsor-validated certificates,
- NCP for Organization, Sponsor, or Individual-validated certificates,
- QCP-n for Individual-validated certificates or
- QCP-l for Organization- validated certificates.

[SMIME] Anwendbare Policies sind:
- LCP für Mail-, Organisations- oder Sponsor-validierte Zertifikate,
- NCP für Organisations-, Sponsor- oder Individual-validierte Zertifikate,
- QCP-n für Individual-validierte Zertifikate,
- QCP-l für Organisations-validierte Zertifikate.

[EVCP] Applicable Policies are EVCP or QEVCP-w.

[EVCP] Anwendbare Policies sind EVCP oder QEVCP-w.

The audits SHALL include all CA certificates. The audit documentation SHALL document all audited PKI hierarchies.

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

[QCP] The Trust Services SHALL be audited according to ETSI EN 319 411-2 in the then current version.

Applicable policies are QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd, QNCP-w or QEVCP-w.

Furthermore, a conformity assessment according to [eIDAS] SHALL be performed

[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, QNCP-w oder QEVCP-w.

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

[3145] The audit process SHALL include the ISMS and the requirements of [TR3145].

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

8.5 Actions taken as a result of deficiency | Maßnahmen infolge von Mängeln

Deficiencies SHALL be corrected within the timelines set by the internal or external auditors.

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

[TLS] [SMIME] Deficiencies that violate the [BR], [EVCG], [MSRP], [MOZRP], [GCRP] or [APLRP] SHALL be

[TLS] [SMIME] Mängel, die gegen die [BR], [EVCG], [MSRP], [MOZRP], [GCRP] oder [APLRP] verstoßen, MÜSSEN den

reported to the affected Root Store operators in accordance with their guidelines. Provided that faulty certificates are complained, the revocation reasons and timelines according to Section 4.9.1 SHALL be taken into account.

betroffenen Root-Store-Betreibern gemäß deren Vorgaben gemeldet werden. Sofern fehlerhafte Zertifikate bemängelt werden, MÜSSEN die Sperrgründe und -fristen gemäß Kap. 4.9.1 berücksichtigt werden.

8.6 Communication of results | Mitteilung der Ergebnisse

No stipulation.

Keine Vorgabe.

[TLS] [SMIME] The links to the audit attestations of all technically unrestricted CAs issued and published by the external auditors SHALL be published in the "Common CA Database" (CCADB).

These attestations SHOULD be published within three months after the end of the audit. In case of a delay of more than three months, a letter of explanation signed by the external auditor SHALL be provided.

When preparing the audit attestations, the external auditors SHALL consider the requirements on form and content from [CCADB#5.1] ("Audit Statement Content", see https://www.ccadb.org/policy).

[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] Conformity Assessment Reports of the audits SHALL be submitted in accordance with Section 8.1.2 to the appropriate supervisory body within three days of receipt.

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

9 Other Business and legal matters | Sonstige geschäftliche und rechtliche Bestimmungen

9.1 Fees | Entgelte

9.1.1 Certificate issuance or renewal fees | Gebühren für die Ausstellung oder Erneuerung von Zertifikaten

No stipulation.

Keine Vorgabe.

9.1.2 Certificate access fees | Gebühren für den Zertifikatszugang

No stipulation.

Keine Vorgabe.

9.1.3 Revocation or status information access fees | Gebühren für den Zugang zu Sperr- oder Statusinformationen

No stipulation.

Keine Vorgabe.

[QCP] Status information SHALL be provided free of charge.

[QCP] Statusinformationen MÜSSEN kostenfrei bereitgestellt werden.

9.1.4 Fees for other services | Gebühren für andere Dienstleistungen

No stipulation.

Keine Vorgabe.

9.1.5 Refund policy | Rückerstattungsrichtlinie

No stipulation.

Keine Vorgabe.

9.2 Financial responsibility | Finanzielle Verantwortlichkeiten

The TSPs SHALL have the financial stability and resources necessary to operate in compliance with this CP, including a planned termination in accordance with Section 5.8. In addition, the TSPs SHALL, to the extent possible under applicable insolvency laws, have arrangements in place to cover the costs of meeting the minimum requirements of Section 5.8 in the event of insolvency.

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 Insurance coverage

TSPs SHALL have adequate liability insurance in accordance with applicable law if they do not have sufficient financial resources to cover any liability claims arising from intentional or negligent acts.

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] The TSPs SHALL have a liability insurance policy with respect to its Trust Services and obligations under this CP as follows:

- a general liability insurance with coverage of at least $2 million
- a professional liability insurance policy with coverage of at least $5 million, which covers claims for damages arising out of
- an act, error or omission
  - an unintentional breach of contract
  - an act of neglect in the issuance or operation of EV certificates
  - a violation of third-party proprietary rights (excluding copyright and trademark violations)
  - a violation of privacy
  - a violation of advertising.

This insurance SHALL be with a company rated no less than "A" in the current edition of "Best's Insurance Guide".

[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 Other assets | Sonstige Vermögensgegenstände

No stipulation.

Keine Vorgabe.

9.2.3 Insurance or warranty coverage for end entities | Versicherungs- oder Garantiedeckung für Endteilnehmer

No stipulation.

Keine Vorgabe.

9.3 Confidentiality of business information | Vertraulichkeit von Geschäftsinformationen

9.3.1 Scope of confidential information | Umfang an vertraulichen Informationen

No stipulation.

Keine Vorgabe.

9.3.2 Information not within the scope of confidential information | Umfang an nicht vertraulichen Informationen

No stipulation.

Keine Vorgabe.

9.3.3 Responsibility to protect confidential information | Verantwortung zum Schutz vertraulicher Informationen

Confidential business information SHALL be protected according to its classification.

Vertrauliche Geschäftsinformationen MÜSSEN ihrer Klassifizierung entsprechend angemessen geschützt werden.

9.4 Privacy of personal information | Schutz von personenbezogenen Daten

9.4.1 Privacy plan | Datenschutzkonzept

The requirements of the General Data Protection Regulation [GDPO] SHALL be complied with.

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

Appropriate technical and organizational measures SHALL be taken
- to maintain integrity and confidentiality during transmission and storage,
- to protect the data against unauthorized or unlawful processing or
- against accidental loss or destruction or damage.

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.

The privacy plans SHALL describe how the provisions of the [GDPO] with regard to the data collected in the registration process are implemented.

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

Data that is not relevant or appropriate to the provision of the service SHALL NOT be collected.

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

The relevant information regarding the processing, storage, deletion and, if applicable, archiving of the collected data, as well as contact information for exercising data protection rights SHALL be published in privacy statements.

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.

The CPS SHALL describe in Section 9.4.1 where the privacy statements can be viewed.

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

9.4.2 Information treated as private | Als privat zu behandelnde Informationen

All personal data that is not to be published in certificates or has already been published elsewhere SHALL be treated as private. This includes information about the true identity of a pseudonym.

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 Information not deemed private | Nicht als privat geltende Informationen

No stipulation.

Keine Vorgabe.

9.4.4 Responsibility to protect private information | Verantwortung für den Schutz privater Informationen

No stipulation.

Keine Vorgabe.

9.4.5 Notice and consent to use private information | Benachrichtigung und Zustimmung zur Verwendung privater Informationen

No stipulation.

Keine Vorgabe.

9.4.6 Disclosure pursuant to judicial or administrative process | Offenlegung im Rahmen eines Gerichts- oder Verwaltungsverfahrens

No stipulation.

Keine Vorgabe.

9.4.7 Other information disclosure circumstances | Andere Umstände der Offenlegung von Informationen

No stipulation.

Keine Vorgabe.

9.5 Intellectual property rights | Urheberrecht

No stipulation.

Keine Vorgabe.

9.6 Representations and warranties | Zusicherungen und Gewährleistungen

9.6.1 CA representations and warranties | Zusicherungen und Gewährleistungen der TSP

The TSPs SHALL be reliable and operate their Trust Services in a trustworthy and legal manner compliant with this CP and their CPSs.

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

The TSPs SHALL retain overall responsibility for compliance with this CP and their CPSs even if they outsource activities to subcontractors or third parties e.g., providers

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

of Trust Service Components or external RAs. To this end, the tasks of the third parties and the associated procedures, responsibilities and liability conditions SHALL be defined and they SHALL be contractually obliged to implement all the required measures. Third party obligations SHALL be described in the CPS.

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.

If Trust Service Components provided by a Trust Service Component Provider are used, it SHALL be ensured that

- the use of the component's interface complies with the requirements specified by the Trust Service Component Provider,
- the security and functionality required by the Trust Service Component comply with the relevant requirements of this CP and the relevant CPSs.

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.

When independent third-party data sources are used to validate data ("QIIS", see Section 3.2.2), they SHALL be evaluated with respect to their reliability, accuracy, and resistance to alteration or falsification. The following SHALL be considered:

- Age of the information provided
- Frequency of updates to the information source
- Data provider and the purpose of the data collection
- Availability of the data
- Integrity of the data (i.e., the relative difficulty of falsifying or altering it)

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)

Databases maintained by the TSP or its affiliates themselves SHALL NOT be considered reliable data sources if the primary purpose of the databases is to collect information to meet validation requirements.

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.

Trust Services SHALL NOT be discriminatory and SHOULD be made available to all applicants,

- whose activities fall within the scope of activities specified by the services and
- who agree to comply with their obligations set forth in the respective terms and conditions.

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.

Trust Services SHALL be made accessible to people with disabilities as far as possible. Applicable accessibility standards from ETSI EN 301 549 SHOULD be taken into account.

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.

Third parties SHALL be given the possibility to validate and test all offered certificate types.

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

[TLS] [SMIME] Telekom Security as the operator of the Root CAs is responsible for

- the services and warranties of the TSP,
- the TSP's compliance with this CP,
- all liabilities and indemnification obligations of the TSP according to [BR].

[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].

For each certificate issued, it SHALL be guaranteed to both the subscribers and the Root Store operators, with whom Telekom Security has an agreement to include the Root CA certificates in the Root Stores, as well as to all relying parties that

- the subscriber has the right to use the domain names, IP addresses or email addresses listed in the subjectDN and/or subjectAltName,
- if applicable, the applicant was authorized to apply for the certificate on behalf of the subscriber,
- the TSP was authorized by the subscribers to issue the certificates,
- the accuracy of all content included in the certificate was validated,
- the subscriber has been identified according to Section 3.2,
- if the subscriber is not affiliated with the TSP, the TSP has entered into a legally valid and enforceable contract with the subscriber that meets all relevant requirements,
- if the subscriber is affiliated with the TSP, a representative of the subscriber has acknowledged the Terms of Use,
- the TSP operates status services in accordance with Section 4.10 at least until the expiration date of the certificates and makes status information available to the public on a 24-hour basis
- the TSP revokes a certificate if one of the reasons for revocation listed in the CPS applies,
- she complies with the requirements of this CP and the respective CPSs during the entire validity period of a certificate

The processes and measures required to comply with the aforementioned certificate guarantees SHALL be described in the CPSs.

The agreements with subscribers including the Terms of Use (see Section 9.6.3) SHALL be legally enforceable.

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 geprüft wurde,
- 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] For each EV certificate issued, it SHALL be ensured that

- the subscriber exists as a legally valid organization, verified with an incorporation or registration agency in the subscriber's incorporation or registration jurisdiction,
- the name of the subscriber at the time of issuance of the certificate is the same as the name in the official registration documents,
- all reasonable steps are taken to verify that
  - the subscriber has the right to use all domain names listed in the certificate at the time of issuance of the certificate,
  - the subscriber has authorized the issuance of the Certificate,
  - all other information in the certificate was correct at the time the certificate was issued,

[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,

- a legally valid and enforceable agreement with a subscriber, that is not affiliated, is concluded, which takes into account all requirements from [EVCG].

- 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] If the private keys of the subscribers are managed by the TSP during the validity period of the corresponding certificates, this SHOULD be described in the CPSs. In addition, this information MAY also be included in the subscriber certificate.

[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] If third parties provide services to a TSP as part of the identification and registration process, a "high" security level for the third parties SHALL be ensured and the reliability of the third party as well as the trustworthiness of the personnel used by the third party SHALL be required. For this purpose, a signed agreement SHALL be concluded with the third party, which in addition also includes the aspects listed in the previous Section.

[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 RA representations and warranties | Zusicherungen und Gewährleistungen der RAs

The representations and warranties of RAs SHALL be defined and described in the CPS, taking into account at least:

- application processing according to Section 4
- organizational measures according to Section 5.2
- personnel measures according to Section 5.3
- archiving of documents according to Section 5.5
- technical measures according to Section 6.5
- privacy requirements according to Section 9.4

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 Subscriber representations and warranties | Zusicherungen und Gewährleistungen der Zertifikatsnehmer

The Terms of Use for subscriber certificates SHALL be defined and the subscribers SHALL have confirmed their acceptance before the certificates are issued.

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

These Terms of Use SHALL consider at least the following obligations of subscribers:

a) an obligation to provide accurate and complete information,
b) an obligation to take all reasonable measures to ensure confidentiality and control over private keys and activation data,
c) an obligation to use the key pair only in accordance with any restrictions communicated to the subscriber,

Diese Nutzungsbedingungen MÜSSEN mindestens folgende Verpflichtungen des Zertifikatsnehmers berücksichtigen:

a) eine Verpflichtung, 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) a prohibition on the unauthorized use of the private subscriber keys,
e) an obligation to revoke or have a certificate revoked without delay if there is a reason for revocation according to Section 4.9.1.2.
f) an obligation to immediately and permanently cease using the private key, except for key decryption (if applicable), after revocation of the subscriber certificate,
g) an obligation to immediately and permanently cease using the private key, except for key decryption (if applicable), once the compromise of the issuing Sub CA has become known,
h) if a subscriber generates its keys itself: An obligation to generate the keys using suitable algorithms and key lengths according to Section 6.1.5,
i) in the case where the subscriber is a natural person and generates its keys itself and these are used for a "signed content commitment" (see Section 7.1.2 (06) regarding KeyUsage "nonRepudiation"): a commitment that the private key is kept under the sole control of the end entity,
j) in the case where the subscriber is a legal person and generates its own keys and uses them for a "signed content commitment" (see Section 7.1.2 (06) regarding KeyUsage „nonRepudiation“): a commitment that the private key is kept under the sole control of the end entity,

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) [TLS] an obligation to install the certificate only on servers that can be accessed under the names listed in the certificate attribute subjectAltName,

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

l) [SMIME] an obligation to use the certificate only for the mailboxes listed in the certificate,

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

m) [TLS] [SMIME] an obligation to verify the content of the certificate for accuracy,
n) [TLS] [SMIME] an obligation to use the certificate only in accordance with all applicable laws and with the concluded agreement and the terms of use,
o) [TLS] [SMIME] an obligation to respond to the TSP's instructions within a specified period of time in the event of compromise of a key or certificate misuse,
p) [TLS] [SMIME] an obligation to accept that the TSP is entitled to revoke a certificate immediately if there is a reason for revocation in accordance with Section 4.9.1.2,

m) [TLS] [SMIME] eine Verpflichtung, den Inhalt des Zertifikats auf Richtigkeit zu überprüfen,
n) [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,
o) [TLS] [SMIME] eine Verpflichtung, innerhalb eines bestimmten Zeitraums auf die Anweisungen des TSP bei Kompromittierung eines Schlüssels oder Zertifikatsmissbrauch zu reagieren,
p) [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,

q) [3145] an obligation to notify the TSP of any change in the registration data and to confirm that the registration data is still valid at the latest after the expiry of the period specified in oo)
r) [3145] if the subscriber generates the keys itself: an obligation to generate and retain the keys in accordance with the specifications (cf. Sections 6.1.5 and 6.1.6),
s) [3145] if the TSP generates and hands over the keys of the subscriber on a token: an obligation to report a compromise of the activation data in the course of token handover, which leads to a revocation of the certificate,
t) [3145] an obligation to verify the subscriber certificate as well as the issuing Sub CA certificate,

u) [QCP-n] an obligation to keep the key under its sole control,
v) [QCP-n] an obligation to use the key only for generating electronic signatures,

w) [QCP-l] an obligation to keep the key under the control of the subject of the certificate,
x) [QCP-l] an obligation to use the key only for the generation of electronic seals.

In addition, the Terms of Use SHALL contain information on the following aspects:
y) if applicable, the applicable policy according to ETSI ,
z) an information what is considered as acceptance of the certificate,
aa) the period for which the records are kept (see Section 5.5.2),
bb) the requirements for relying parties according to Section 9.6.4,
cc) whether, and if so in what way, the requirements of this CP will be supplemented or further restricted,
dd) any restrictions on the use of the services provided,
ee) the limitations of liability of the TSP,
ff) the applicable law,
gg) the procedures for complaints and dispute resolution,
hh) frequency and applicable audit schemes of the audits of the TSP according to Sections 8.1 and 8.4,
ii) contact information of the TSP,
jj) statements on the availability of the services provided,
kk) the revocation reasons to be chosen in the event of revocation by the subscriber,

ll) [3145] the way in which the subscribers can transmit the registration data,
mm) [3145] regulations on the acceptance of new versions of the Terms of Use by the subscribers in accordance with the applicable laws,
nn) [3145] a definition of the various roles of the subscribers, the various possible subjects of a certificate and other significant roles in the certificate management processes (see Section 1.3.3)

q) [3145] eine Verpflichtung, jede Änderung der Registrierungsdaten dem TSP mitzuteilen und spätestens nach Ablauf der unter oo) festgelegten Frist zu bestätigen, dass die Registrierungsdaten noch gültig sind,
r) [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),
s) [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,
t) [3145] eine Verpflichtung, das Endteilnehmer-Zertifikat sowie das ausstellende Sub-CA-Zertifikat zu prüfen,

u) [QCP-n] eine Verpflichtung, den Schlüssel unter seiner alleinigen Kontrolle zu halten,
v) [QCP-n] eine Verpflichtung, den Schlüssel ausschließlich zur Erzeugung elektronischer Signaturen zu nutzen,

w) [QCP-l] eine Verpflichtung, den Schlüssel unter der Kontrolle der Organisation zu halten,
x) [QCP-l] eine Verpflichtung, den Schlüssel ausschließlich zur Erzeugung elektronischer Siegel zu nutzen.

Darüber hinaus MÜSSEN die Nutzungsbedingungen Informationen zu folgenden Aspekten enthalten:
y) sofern anwendbar, die anwendbare Policy gemäß ETSI
z) eine Information, was als Akzeptanz des Zertifikats gilt
aa) der Zeitraum, über den die Aufzeichnungen (siehe Kap. 5.5.2) aufbewahrt werden
bb) Anforderungen an vertrauende Dritte gemäß Kap. 9.6.4
cc) ob und wenn ja, auf welche Art und Weise die Anforderungen dieser CP ergänzt oder weiter eingeschränkt werden
dd) alle Beschränkungen der Nutzung des angebotenen Dienstes
ee) Haftungsbeschränkungen der TSP
ff) anwendbares Recht
gg) Verfahren bei Beschwerden und zur Streitbeilegung
hh) Häufigkeit und zugrundeliegende Auditschemata der Auditierungen der TSP gemäß Kap. 8.1 und 8.4
ii) Kontaktinformationen des TSP
jj) Aussagen zur Verfügbarkeit der bereitgestellten Dienste
kk) auszuwählende Sperrgründe bei Sperrung durch den Zertifikatsnehmer

ll) [3145] die Art und Weise, wie die Zertifikatsnehmer die Registrierungsdaten übertragen können,
mm) [3145] Regelungen zur Akzeptanz neuer Versionen der Nutzungsbedingungen durch die Zertifikatsnehmer außerhalb der Antragsprozesse in Übereinstimmung mit den geltenden Gesetzen,
nn) [3145] eine Definition der verschiedenen Rollen der Zertifikatsnehmer, der verschiedenen möglichen Subjekte

oo) [3145] a time limit after which subscribers must confirm, that the registration data is still valid,
pp) [3145] further requirements for subscribers depending on the required security level (e.g., virus protection, firewalls as well as security updates of operating systems, adequate protection of keys and activation data, use of secure cryptographic modules in case of high security level),
qq) [3145] if the subscriber generates the keys itself: the requirements for the hardware and software used to generate the keys,
rr) [3145] if the TSP generates subscriber keys: the process of handing over the keys,
ss) [3145] if the TSP generates and hands over subscriber keys on token: the process of handing over the token,
tt) [3145] the requirements for certificate renewal with or without key change and for issuing a replacement certificate,
uu) [3145] The periods and circumstances under which modification of certificate data is permitted or required,
vv) [3145] information about the process of termination according to Section 5.8,
ww) [3145] information about the periods of the regular updates of the status services.

eines Zertifikats, sowie weiterer bedeutender Rollen in den Zertifikatsmanagementprozessen (siehe Kap. 1.3.3),
oo) [3145] eine Frist, nach deren Ablauf die Zertifikatsnehmer bestätigen müssen, dass ihre Registrierungsdaten weiterhin gültig sind,

pp) [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),
qq) [3145] für den Fall, dass ein Zertifikatsnehmer die Schlüssel selbst generiert: die Anforderungen an die zur Schlüsselgenerierung verwendete Hard- und Software,
rr) [3145] für den Fall, dass die TSP die Schlüssel der Zertifikatsnehmer generieren: der Prozess der Schlüsselübergabe,
ss) [3145] für den Fall, dass die TSP die Schlüssel der Zertifikatsnehmer auf Token generieren und übergeben: der Prozess der Übergabe der Token,
tt) [3145] die Voraussetzungen für eine Zertifikatserneuerung mit oder ohne Schlüsselwechsel sowie für die Ausstellung eines Ersatzzertifikats,
uu) [3145] Die Zeiträume und Umstände, unter denen eine Änderung von Zertifikatsdaten erlaubt oder erforderlich ist,
vv) [3145] Informationen über den Prozess der Beendigung eines TSP oder einer RA (siehe Kap. 5.8),
ww) [3145] Informationen über die Fristen der regelmäßigen Updates der Statusdienste.

xx) [VS-NfD] Classification of key material according to [SÜG] and [VSA].

xx) [VS-NfD] Einstufung des Schlüsselmaterials nach [SÜG] und [VSA].

yy) [QCP] The time in which the status services are provided after the expiration of the certificates,
zz) [QCP] whether revoked certificates will be listed in the revocation lists after expiration and how this is indicated in the revocation lists,
aaa) [QCP] the circumstances under which a CA ceases to issue revocation lists and the format of the last revocation list issued by that CA,
bbb) [QCP] the usage of the extension `archiveCutOff`.

yy) [QCP] Die Zeit, in der die Statusdienste nach Ablauf der Zertifikate bereitgestellt werden,
zz) [QCP] ob gesperrte Zertifikate nach ihrem Ablauf weiterhin in den Sperrlisten aufgeführt werden und wie dies in den Sperrlisten gekennzeichnet ist,
aaa) [QCP] die Umstände, wenn eine CA die Ausstellung von Sperrlisten beendet sowie das Format der letzten von dieser CA ausgestellten Sperrliste,
bbb) [QCP] die Nutzung der Erweiterung `archiveCutOff`.

The Terms of Use MAY be provided in the form of a PDS according to [ETS411-1#Annex A].

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

9.6.4 Relying party representations and warranties | Zusicherungen und Gewährleistungen der Zertifikatsnutzer

The following recommendations for relying parties SHALL be included in the Terms of Use (see also Section 9.6.3) and/or the PDS.

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

Relying parties SHOULD

- check the validity of the certificates via the offered status services according to Section 4.9.10 and 4.10,
- consider the restrictions on the use of the certificates set out in the terms of use or in the certificate,
- take all further precautions arising for third parties from agreements or other regulations.

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 Representations and warranties of other participants | Zusicherungen und Gewährleistungen sonstiger Teilnehmer

No stipulation.

Keine Vorgabe.

9.7 Disclaimers of warranties | Gewährleistungsausschlüsse

No stipulation.

Keine Vorgabe.

9.8 Limitations of liability | Haftungsbeschränkungen

The liability of the TSP MAY be limited in accordance with applicable law. The limitations of liability SHALL be described in the CPSs as well as in the Terms of Use, see also Section 9.6.3 para. ee).

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. ee).

[EVCP] The liability to subscribers or relying parties for legally recognized and provable claims SHALL NOT be limited to a monetary amount of less than two thousand U.S. dollars per subscriber or relying party per subscriber certificate.

[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] The TSP SHALL be liable under Article 13 of EU Regulation 910/2014 ("eIDAS") for any damage caused intentionally or negligently to a natural or legal person.

[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 Indemnities | Schadensersatz

No stipulation.

Keine Vorgabe.

9.10 Term and termination of this CP or a CPS | Laufzeit und Aufhebung dieser CP oder eines CPS

9.10.1 Term | Laufzeit

This CP and all CPSs based on it have a maximum validity period of one year, see also Section 9.12.

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

9.10.2 Termination | Aufhebung

No stipulation.

Keine Vorgabe.

9.10.3 Effect of termination and survival | Auswirkungen der Beendigung und Fortführung

No stipulation.

Keine Vorgabe.

9.11 Individual notices and communications with participants | Individuelle Mitteilungen und Kommunikation mit Teilnehmern

No stipulation.

Keine Vorgabe.

9.12 Amendments to this CP or a CPS | Änderungen an dieser CP oder einem CPS

9.12.1 Procedure for amendment | Verfahren für Änderungen

This CP SHALL be reviewed by the Trust Center's PKI Compliance Management as needed, e.g., due to changed requirements or relevant changes in operations, but at the latest within one year after the effective date.

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.

The PKI Compliance Management SHALL therefore regularly review, at appropriate intervals, the underlying requirements of the documents referenced in Annex B for new versions and monitor the activities in relevant forums.

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.

Changes to this CP as well as the annual review SHALL be listed in the revision history of this document. This applies even if no substantive changes are made at the annual review.

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.

New versions of this CP SHALL be approved according to Section 1.5.4 and shall be assigned a new ascending version number.

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

Similarly, the CPSs SHALL be reviewed by the Trusted Services due to changed requirements or relevant changes in operation, but at least once per year. Regarding the change history, approval procedure and versioning, the above applies.

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.

If changes are made to the CPS that affect the Terms of Use, the Terms of Use SHALL be amended and provided in a new version.

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 Notification mechanism and period | Benachrichtigungsmechanismus und -zeitraum

New versions of this CP SHALL be published according to the specifications of Section 2.2. All affected Trusted Services SHALL be informed at the latest when a new version is published.

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.

New versions of a CPS or the Terms of Use SHALL be published according to the specifications of Section 2.2. At the latest with the release of a new version, all affected Trust Service staff SHALL be informed.

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.

The subscribers and, if applicable, relying parties SHALL be informed about new versions of the Terms of Use if they contain new or changed conditions that also affect the use of already issued certificates or keys. When announcing the changes, reference MAY be made to the changed documents in the repository with regard to the details.

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] Acceptance of new Terms of Use, which contain new or modified conditions that also affect the use of already issued certificates or keys, SHALL be obtained from the subscriber. Regarding the regulations for the acceptance of new Terms of Use besides the application processes, see Section 9.6.3 pp).

[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] New versions of a CPS SHALL be communicated to the supervisory authorities.

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

9.12.3 Circumstances under which OID must be changed | Umstände, unter denen die OID geändert werden muss

If there are changes to this CP or to a CPS that affect the applicability of the respective document, the document SHOULD be given a new OID.

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 Dispute resolution provisions | Bestimmungen zur Beilegung von Streitigkeiten

Policies and procedures for resolving complaints and disputes received from subscribers or relying parties regarding the Trust Services SHALL be established and described in the CPSs and Terms of Use.

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 Governing law | Geltendes Recht

German law SHALL be set as the applicable law in the CPSs.

In den CPS MUSS das deutsche Recht als geltendes Recht festgelegt werden.

9.15 Compliance with applicable law | Einhaltung geltenden Rechts

The TSP SHALL ensure that they comply with applicable law and provide evidence of how they comply with applicable legal requirements as needed.

Die TSP MÜSSEN sicherstellen, dass sie geltendes Recht einhalten und bei Bedarf Nachweise darüber vorlegen, wie sie die geltenden rechtlichen Anforderungen erfüllt.

9.16 Miscellaneous provisions | Verschiedene Bestimmungen

9.16.1 Entire agreement | Gesamte Vereinbarung

No stipulation.

Keine Vorgabe.

9.16.2 Assignment | Zuordnung

No stipulation.

Keine Vorgabe.

9.16.3 Severability | Salvatorische Klausel

No stipulation.

Keine Vorgabe.

[TLS] [SMIME] In the case of a conflict between [BR] or [SBR] and a law, any conflicting requirement MAY be modified to the extent necessary to make the requirement valid and legal. This applies only to operations or certificate issuances subject to this law. In such a case, a detailed reference to the law requiring modification of those requirements under this section SHALL be given in the CPS, as well as the specific modification of those requirements made by the TSP. Before issuing a certificate under the modified requirements, the CA/Browser Forum SHALL be informed of the relevant passages of the modified Section (see [BR#9.16.3] resp. [SBR#16.3]).

Modifications made SHALL be ceased as soon as the law relied upon for that modification is no longer in effect or the requirements of the [BR] or [SBR] have been modified to make it possible to comply with them and the law at the same time. An appropriate change in practice, a change in the respective CPSs, and notification to the CA/Browser Forum SHALL be made within 90 days.

[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 Enforcement (attorneys' fees and waiver of rights) | Rechtsdurchsetzung

No stipulation.

Keine Vorgabe.

9.16.5 Force Majeure | Höhere Gewalt

No stipulation.

Keine Vorgabe.

9.17 Other provisions | Sonstige Bestimmungen

No stipulation.

Keine Vorgabe.

Appendix | Anhang

Appendix A: Abbreviations | Anhang A: Abkürzungen

Note: Due to international standardization, the abbreviations usually refer to English technical terms, which will not be translated into German at this point.

Hinweis: Aufgrund der internationalen Standardisierung verbergen sich hinter den Abkürzungen meist englische Fachbegriffe, auf deren Übersetzung in die deutsche Sprache hier verzichtet wird.

Table 4 – Abbreviations | Tabelle 4 – Abkürzungen

Abbreviation | Abkürzung	Meaning | Bedeutung
AATL	Adobe Approved Trust List
ADN	Authorization Domain Name
ARL	Authority Revocation List (see 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)
DBA	Doing Business As
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
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 (deprecated)
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
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 Resource Locator
UTC	Coordinated Universal Time
VDG	Vertrauensdienstegesetz
VDV	Vertrauensdiensteverordnung
VSA	Verschlusssachenanweisung
VS-NfD	„Verschlusssache - Nur für den Dienstgebrauch“ (German Federal secrecy instruction)

Appendix B: References | Anhang B: Referenzen

Table 5 – References | Tabelle 5 - Refrenzen

Reference | Referenz	Referenced Document | Referenziertes Dokument
[ADTL]	Adobe Approved Trust-List Tech. Requirements
[APRP]	Apple Root Certificate Program
[APCT]	Apple's Certificate Transparency policy
[BR]	CAB-Forum Baseline Requirements
[CCADB]	CCADB Policy
[eIDAS]	eIDAS (Regulation (EU) No. 910/2014 of the European Parliament and of the Council)
[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 Certificate Profile
[GCTL]	Google Certificate Transparency Log Policy
[MSRP]	Microsoft Trusted Root Program
[MOZRP]	Mozilla Root Store Policy
[MOZCA]	Mozilla CA/Application Process
[NCSSR]	CAB-Forum Network Security Guidelines
[SÜG]	„Sicherheitsüberprüfungsgesetz“ (German Law)
[TR3145]	Technical Guideline | Technische Richtlinie TR-03145-1, Secure CA operation Part 1, German Federal Office for Information Security | Bundesamt für die Sicherheit in der Informationstechnik
[TR3145VS]	Technical Guideline | Technische Richtlinie TR-03145-VS-NfD, Secure CA operation VS-NfD, German Federal Office for Information Security | Bundesamt für die Sicherheit in der Informationstechnik
[VDG]	„Vertrauensdienstegesetz“ (German Law)
[VDV]	„Vertrauensdiensteverordnung“ (German Law)
[VSA]	„Verschlusssachenanweisung des Bundes“ (German Federal secrecy instruction)
[X500]	ITU-T X.500 Serie / ISO/IEC 9594 Serie Information technology - Open systems interconnection - The Directory

Appendix C: Definitions | Anhang C: Definitionen

Notes:

- At this point, it is omitted from listing again known definitions of internationally established terms in the PKI environment; in this respect, reference is made to the definitions of the ETSI specifications and RFCs listed in Appendix B. In the following, terms are defined that are used specifically for certain certificate types, and some terms used in this document whose usage may differ between the German and English languages are clarified.
- For the sake of clarity, the definitions in English and then the definitions in German are listed in separate tables below.

Hinweise:

- 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.
- Nachfolgend werden der Übersichtlichkeit halber zunächst die Definitionen in englischer Sprache und anschließend die Definitionen in deutscher Sprache in separaten Tabellen aufgeführt.

Table 6a – Definitions in English

Term	Definition
Advanced electronic seal	Electronic seal according to [eIDAS#Art.36]
Advanced electronic signature	Electronic signature according to [eIDAS#Art.26]
Certification Authority Authorization (CAA)	DNS resource record that allows the owner of a DNS domain name to specify the TSPs that are authorized to issue certificates for that domain
High-Risk Certificate Request	Certificate applications the TSP flags for additional review based on internal criteria. These may include: ▪ mixed character domain names ▪ names that are at higher risk for phishing or other fraudulent use, ▪ names included in previously rejected certificate requests or revoked certificates, ▪ names listed on the Miller Smiles phishing list or the Google Safe Browsing list; or ▪ names that a TSP identifies based on their own risk mitigation criteria.
Leaf Certificate	A TLS certificate that was previously published as a pre-certificate
Non-Reserved LDH-Label	Component of a domain name that does not have a '-' in the third and fourth positions
P-Label	Component of a domain name that has a '-' in the third and fourth positions ("XN label") and is followed from the fifth position by a valid output of the punycode algorithm according to [RFC3492# 6.3]
Pre-Certificate	Certificate according to [RFC6962] for public logging of a yet-to-be-issued TLS certificate. The pre-certificate is generated from the yet-to-be-issued certificate (exact 1:1 copy) plus the special critical extension Certificate Transparency precertificate poison extension (OID 1.3.6.1.4.1.11129.2.4.3) and signed by the CA, which will also sign the leaf certificate later. Pre-Certificates are not considered certificates according to [RFC5280] and cannot be validated by standard X.509v3 clients. The (real) TLS certificate generated later from the Pre-certificate is called a *Leaf Certificate*.
Pseudonym	Fictitious identity that a person assumes for a specific purpose and that is different from his or her original or true identity. NOTE: A pseudonymous identity, unlike an anonymous identity, can be linked to the person's true identity. The true identity is known to the TSP
Signed Certificate Timestamp (SCT)	Return value of a CT log server according to [RFC6962] to a pre-certificate published there by the TSP. All SCTs returned on the publication of a pre-certificate in different CT-Log servers are included in the Leaf certificate in the signedCertificateTimestampList extension.
Token	Hardware module that generates and/or handles cryptographic keys in a secure manner

Verified method of communication	The use of a telephone number, fax number, email address, or postal address that has been verified by a TSP as a reliable way of communicating with the *Applicant* in accordance with [EVCG#11.5]
Verschlusssache - Nur für den Dienstgebrauch	A classification of German government information to be protected
Wildcard Certificate	A certificate with a *Wildcard Domain Name*
Wildcard Domain Name	A domain name consisting of a single asterisk followed by a single dot ("*.") followed by a FQDN.

Tabelle 7b – Definitionen in Deutsch

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 IANA 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 und von der CA signiert, die auch später das Leaf-Zertifikat signiert. 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

Appendix D: Certificate Profiles | Anhang D: Zertifikatsprofile

Below, the mandatory and optional extensions and `subjectDN` attributes of some certificate types are listed.

Extensions and attributes not listed there SHALL NOT be set.

NOTE: The certificate profiles listed below only apply to certificates issued in accordance with ETSI and/or the requirements of the CA/Browser Forum. These certificate profiles do not apply to certificates issued in accordance with [TR3145], with the exception of the OCSP signer certificate profile. In this regard, please refer to the relevant specifications for the trust services concerned.

Nachfolgend werden die obligatorischen und optionalen Erweiterungen und `subjectDN`-Attribute einzelner Zertifikatstypen aufgeführt.

Dort nicht aufgeführte Erweiterungen und Attribute DÜRFEN NICHT gesetzt werden.

HINWEIS: Die nachfolgend aufgeführten Zertifikatsprofile beziehen sich nur auf Zertifikate, die gemäß ETSI und/oder den Vorgaben des CA/Browser-Forums ausgestellt werden. Für Zertifikate, die gemäß [TR3145] ausgestellt werden, gelten diese Zertifikatsprofile, mit Ausnahme des Profils der OCSP-Signer-Zertifikate, nicht. Diesbezüglich sei auf die einschlägigen Vorgaben zu den betroffenen Trust Servcies verwiesen.

D1: Root Certificates | Root-CA-Zertifikate

The following attributes of the `subjectDN` SHALL be set:
- `commonName`
- `organizationName`
- `countryName`

The following extensions SHALL be set:
- `subjectKeyIdentifier`
- `keyUsage`
- `basicConstraints`

The following extension MAY be set:
- `authorityKeyIdentifier`

Folgende Attribute des `subjectDN` MÜSSEN gesetzt werden:
- `commonName`
- `organizationName`
- `countryName`

Folgende Erweiterungen MÜSSEN gesetzt werden:
- `subjectKeyIdentifier`
- `keyUsage`
- `basicConstraints`

Folgende Erweiterung DARF gesetzt werden:
- `authorityKeyIdentifier`

D2: Sub-CA Certificates | Sub-CA-Zertifikate

The following attributes of the `subjectDN` SHALL be set:
- `commonName`
- `organizationName`
- `countryName`
- `organizationIdentifier`

The following extensions SHALL be set:
- `subjectKeyIdentifier`
- `keyUsage`
- `basicConstraints`
- `authorityKeyIdentifier`
- [TLS] [SMIME] `certificatePolicies`
- [TLS] [SMIME] `extendedKeyUsage`
- [TLS] [SMIME] `cRLDistributionPoints`
- [TLS] [SMIME] `authorityInfoAccess`

Folgende Attribute des `subjectDN` MÜSSEN gesetzt werden:
- `commonName`
- `organizationName`
- `countryName`
- `organizationIdentifier`

Folgende Erweiterungen MÜSSEN gesetzt werden:
- `subjectKeyIdentifier`
- `keyUsage`
- `basicConstraints`
- `authorityKeyIdentifier`
- [TLS] [SMIME] `certificatePolicies`
- [TLS] [SMIME] `extendedKeyUsage`
- [TLS] [SMIME] `cRLDistributionPoints`
- [TLS] [SMIME] `authorityInfoAccess`

The following extensions SHOULD be set:
- cRLDistributionPoints
- authorityInfoAccess
- [QCP] validityModel

[TLS] [SMIME] The above requirements apply to Sub-CA certificates. For cross certificates the requirements from [BR] or [SBR] SHALL be considered.

Folgende Erweiterungen DÜRFEN 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.

D3: OCSP-Signer Certificates | OCSP-Signer-Zertifikate

The following attributes of the subjectDN SHALL be set:
- commonName
- countryName
- organizationName

The following extensions SHALL be set:
- authorityKeyIdentifier
- keyUsage
- extendedKeyUsage
- id-pkix-ocsp-nocheck

The following extension SHOULD be set:
- subjectKeyIdentifier

The following extension MAY be set:
- basicConstraints

Folgende Attribute des subjectDN MÜSSEN gesetzt werden:
- commonName
- countryName
- organizationName

Folgende Erweiterungen MÜSSEN gesetzt werden:
- authorityKeyIdentifier
- keyUsage
- extendedKeyUsage
- id-pkix-ocsp-nocheck

Folgende Erweiterung SOLLTE gesetzt werden:
- subjectKeyIdentifier

Folgende Erweiterung DARF gesetzt werden:
- basicConstraints

D4: Subscriber Certificates | Endteilnehmer-Zertifikate

[ETSI] The following ETSI specifications are relevant for the issuance of subscriber certificates:
- Certificates for natural persons SHALL be issued according to [ETS412-2], the specific implementation for S/MIME certificates is listed in Annex D4.2.
- Certificates for organizations SHALL be issued according to [ETS412-3], the specific implementation for S/MIME certificates is listed in Annex D4.2.
- Certificates for websites SHALL be issued according to [ETS412-4], the specific implementation for TLS certificates is listed in Annex D4.1

The generic requirements for certificates for natural persons and organizations are listed in Annex D4.3.

[ETSI] Für die Ausstellung von Endteilnehmer-Zertifikaten sind folgende ETSI-Spezifikationen relevant:
- Zertifikate für natürliche Personen MÜSSEN gemäß [ETS412-2] ausgestellt werden, die konkrete Umsetzung für S/MIME-Zertifikate ist in Anhang D4.2 aufgeführt.
- Zertifikate für Organisationen MÜSSEN gemäß [ETS412-3] ausgestellt werden, die konkrete Umsetzung für S/MIME-Zertifikate ist in Anhang D4.2 aufgeführt.
- Zertifikate für Webseiten MÜSSEN gemäß [ETS412-4] ausgestellt werden, die konkrete Umsetzung für TLS-Zertifikate ist in Anhang D4.1 aufgeführt

Die generischen Anforderungen an Zertifikate für natürliche Personen und Organisationen sind in Anhang D4.3 aufgeführt.

[TLS] The following attributes of the `subjectDN` SHALL be set:
- `commonName`

In Organization Validated Certificates the following attributes SHALL be set additionally:
- `countryName`
- `stateOrProvinceName`, if `localityName` is not set
- `localityName`, if `stateOrProvinceName` is not set
- `organizationName`

In Organization Validated Certificates the following attributes MAY be set additionally:
- `postalCode`
- `streetAddress`
- `stateOrProvinceName`
- `localityName`

[TLS] Folgende Attribute des `subjectDN` MÜSSEN gesetzt werden:
- `commonName`

In Organisations-validierten Zertifikaten MÜSSEN darüber hinaus folgende Attribute des subjectDN gesetzt werden:
- `countryName`
- `stateOrProvinceName`, wenn `localityName` nicht gesetzt wird
- `localityName`, wenn `stateOrProvinceName` nicht gesetzt wird
- `organizationName`

In Organisations-validierten Zertifikaten DÜRFEN darüber hinaus folgende Attribute gesetzt werden:
- `postalCode`
- `streetAddress`
- `stateOrProvinceName`
- `localityName`

[EVCP] In addition, the following attributes of the `subjectDN` SHALL be set:
- `businessCategory`
- `jurisdictionOfIncorporationCountryName`
- `jurisdictionOfIncorporationStateOrProvinceName` if the registration authority acts at the state or local level, otherwise it SHALL NOT be set
- `jurisdictionOfIncorporationLocalityName` if the registration authority acts on the local level, otherwise it SHALL NOT be set
- `serialNumber`

The following attribute of the `subjectDN` MAY be set:
- `organizationIdentifier`

[EVCP] Ergänzend MÜSSEN folgende Attribute des `subjectDN` gesetzt werden:
- `businessCategory`
- `jurisdictionOfIncorporationCountryName`
- `jurisdictionOfIncorporationStateOrProvinceName`, wenn die Registrierungsinstanz auf Ebene eines Bundeslands oder auf kommunaler Ebene agiert, ansonsten DARF er NICHT gesetzt werden.
- `jurisdictionOfIncorporationLocalityName`, wenn die Registrierungsinstanz auf kommunaler Ebene agiert, ansonsten DARF er NICHT gesetzt werden.
- `serialNumber`

Folgendes Attribut des `subjectDN` DARF gesetzt werden:
- `organizationIdentifier`

[QCP] Deviating from [OVCP] and [EVCP], the following attributes of the subjectDN SHALL be set:
- `localityName`
- `organizationIdentfier`

[QCP] Abweichend zu [OVCP] und [EVCP] MÜSSEN folgendes Attribute des subjectDN gesetzt werden:
- `localityName`
- `organizationIdentfier`

[TLS] The following extensions SHALL be set:
- `authorityKeyIdentifier`
- `keyUsage`
- `certificatePolicies`
- `subjectAltName`
- `extendedKeyUsage`
- `cRLDistributionPoints`
- `authorityInfoAccess`
- `signedCertificateTimestampList`

[TLS] Folgende Erweiterungen MÜSSEN gesetzt werden:
- `authorityKeyIdentifier`
- `keyUsage`
- `certificatePolicies`
- `subjectAltName`
- `extendedKeyUsage`
- `cRLDistributionPoints`
- `authorityInfoAccess`
- `signedCertificateTimestampList`

In pre-certificates the follwoing extension SHALL be set additionally:
- precertificate poison extension

The following extensions MAY be set:
- subjectKeyIdentifier
- basicConstraints

In Pre-Zertifikaten MUSS zusätzlich folgende Erweiterung gesetzt werden:
- precertificate poison extension

Folgende Erweiterungen DÜRFEN gesetzt werden:
- subjectKeyIdentifier
- basicConstraints

[EVCP] In addition to [TLS], the CABFOrganizationIdentifier extension SHALL be set if the organizationIdentifier is set, otherwise it SHALL NOT be set.

[EVCP] Ergänzend zu [TLS] MUSS die Erweiterung CABFOrganizationIdentifier gesetzt werden, wenn der organizationIdentifier gesetzt ist, ansonsten DARF sie NICHT gesetzt werden.

[QCP] The qcStatements extension SHALL be set.

[QCP] Es MUSS zusätzlich qcStatements gesetzt werden.

D4.2: S/MIME Certificates | S/MIME-Zertifikate

[SMIME] The following attribute of the subjectDN SHALL be set:
- commonName

The following attributes MAY be set:
- serialNumber
- emailAddress

The following attribues MAY be set additionally in all certificates with the exception of Mail-validated certificates:
- localityName (if countryName is set)
- stateOrProvinceName (if countryNameis set)
- streetAddress (if localityName is set)
- postalCode (if countryName is set)
- countryName

In Organization Validated Certificates, the following attributes SHALL be set in addition to [SMIME]:
- organizationName
- organizationIdentifier

In Sponsor Validated Certificates, the following attributes SHALL be set in addition to [SOV]:
- surname und givenName oder pseudonym

In Individual Validated Certificates, the following attributes SHALL be set in addition to [SMIME]:
- surname und givenName oder pseudonym

[SMIME] Folgendes Attribut des subjectDN MUSS gesetzt werden:
- commonName

Folgende Attribute DÜRFEN gesetzt werden:
- serialNumber
- emailAddress

Folgende Attribute DÜRFEN darüber hinaus bei allen Zertifikatstypen mit Ausnahme von Mail-validierten Zertifikaten gesetzt werden:
- localityName (sofern countryName gesetzt ist)
- stateOrProvinceName (sofern countryName gesetzt ist)
- streetAddress (sofern localityName gesetzt ist)
- postalCode (sofern countryName gesetzt ist)
- countryName

In Organisations-validierten Zertifikaten MÜSSEN ergänzend zu [SMIME] folgende Attribute gesetzt werden:
- organizationName
- organizationIdentifier

In Sponsor-validierten Zertifikaten MÜSSEN ergänzend zu [SOV] folgende Attribute gesetzt werden:
- surname und givenName oder pseudonym

In Individual-validierten Zertifikaten MÜSSEN ergänzend zu [SMIME] folgende Attribute gesetzt werden:
- surname und givenName oder pseudonym

[SMIME] The following extensions SHALL be set:
- certificatePolicies
- cRLDistributionPoints
- authorityInformationAccess
- keyUsage

[SMIME] Folgende Erweiterungen MÜSSEN gesetzt werden:
- certificatePolicies
- cRLDistributionPoints
- authorityInformationAccess
- keyUsage

- extKeyUsage
- authorityKeyIdentifier
- subjectAlternativeName
- subjectKeyIdentifier
- [QCP] qcStatement

The following extension MAY be set:
- basicConstraints

- extKeyUsage
- authorityKeyIdentifier
- subjectAlternativeName
- subjectKeyIdentifier
- [QCP] qcStatement

Folgende Erweiterung DARF gesetzt werden:
- basicConstraints

D4.3: Generic Certificate Profiles according to ETSI | Generische Zertifikatsprofile gemäß ETSI

[ETSI] The following attributes of the subjectDN SHALL be set in certificates for natural persons not related to an organization:
- countryName
- commonName
- surname and givenName or pseudonym
- serialNumber if the other attributes of the subjectDN do not ensure uniqueness

In addition, the attributes listed in Table 3, which do not refer to organizations, MAY be set.

[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] The following attributes of the subjectDN SHALL be set in certificates for natural persons related to an organization:
- countryName
- commonName
- surname and givenName or pseudonym
- organizationName
- serialNumber if the other attributes of the subjectDN do not ensure uniqueness.

In addition, the attributes listed in Table 3 MAY be set.

[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] The following attributes of the subjectDN SHALL be set in certificates for organizations:
- countryName
- organizationName
- organizationIdentifier
- commonName

In addition, the attributes listed in Table 3, which do not refer to natural persons, MAY be set.

[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.

[ETSI] The following extensions SHALL be set as a minimum in certificates for natural persons or organizations:
- authorityKeyIdentifier
- keyUsage
- certificatePolicies
- authorityInfoAccess

[ETSI] Folgende Erweiterungen MÜSSEN in Zertifikaten für natürliche Personen oder Organisationen mindestens gesetzt werden:
- authorityKeyIdentifier
- keyUsage
- certificatePolicies
- authorityInfoAccess

- `cRLDistributionPoints`, if applicable (see Section 7.1.2 (31))
- [QCP] `QCStatement`

The following extension SHOULD be set in certificates for natural persons or organizations:

- `subjectKeyIdentifier`

In addition, the extensions listed in Table 2 MAY be set.

- ggf. `cRLDistributionPoints` (siehe Kap. 7.1.2 (31))
- [QCP] `qcStatement`

Folgende Erweiterung SOLLTE in Zertifikaten für natürliche Personen oder Organisationen gesetzt werden:

- `subjectKeyIdentifier`

Darüber hinaus DÜRFEN die in Tabelle 2 aufgeführten Erweiterungen gesetzt werden.