Deutsche Telekom Security GmbH
CPS TeleSec ServerPass

Öffentlich

Version: 16.00

Gültig ab: 30.04.2021

Status: Freigabe

Letztes Review: 28.04.2021

Impressum

Tabelle 1: Impressum

Angaben	Ausprägung
Herausgeber	Deutsche Telekom Security GmbH Trust Center & ID-Solutions, Chapter Trust Center Products Untere Industriestraße 20, 57250 Netphen, Deutschland
Dateiname	CPS_TeleSec_ServerPass_DE_V16.00.docx
Gültig ab	30.04.2021
Titel	CPS TeleSec ServerPass
Version	16.00
Letztes Review	28.04.2021
Status	Freigabe
Autor	Telekom Security
Inhaltlich geprüft von	Telekom Security
Freigegeben von	Telekom Security
Beteiligte Organisationseinheit	Telekom Security Trust Center & ID-Solutions
Ansprechpartner	Telekom Security Leiter Trust Center Betrieb
Kurzbeschreibung	Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement - CPS)

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen / Kommentar
1.0	28.11.2000	DB	Initialversion
2.0	01.09.2001	LE	Aufnahme Erneuerung
3.0	11.11.2003	LE	Aktualisierung der Zertifikatshierarchie, Überarbeitung inhaltlich, Layoutänderungen
3.4	04.05.2007	LE	Layoutanpassung, Aktualisierung Kapitel 14
Zusammenlegung der Produkte TeleSec ServerPass Standard und TeleSec ServerPass EV (Extended Validation) und damit die Zusammenlegung in einem neuen Dokument CP/CPS.			
1.0	14.04.2010	LEI, SK, UV	Ersetzt CPS_ServerPass_V3.4 und CPS_ServerPass_EV_V1.0 Aufbau nach RFC3647, alle Kapitel wurden überarbeitet und Inhalte entsprechend aktualisiert, Layoutanpassung.
2.0	01.07.2013	UV; MG, LE	Das gesamte Dokument überarbeitet, detailliert und erweitert.
3.0	25.03.2015	UV, LE, MB, ME	Das gesamte Dokument überarbeitet, aktualisiert, detailliert und erweitert. QS und Freigabe
4.0	14.04.2016	LE, MB, LR ME, AT	Im Rahmen des Dokumentreviews überarbeitet und aktualisiert QS und Freigabe
5.0	19.04.2017	LR, MB, LEI ME. AT	Erweiterungen für eIDAS hinzugefügt, Kap. 6.1.5 aktualisiert, Kap. 4.2.3 ergänzt. Kapitel 5.7.1 ergänzt, Kap. 6.5.1 und 6.5.1.1 ergänzt, Kap. 6.1.1 und Kap. 5.4.8 ergänzt, Kap. 1.3.1 ergänzt, EV um EV SAN ergänzt, Kap. 4.11 ergänzt QS und Freigabe
6.0	28.03.2018	AR	QS zur Freigabe Nach Freigabe durch ME
7.0	13.04.2018	LE	Nach Freigabe durch ME
8.0	02.08.2018	GK	Nach Freigabe durch ME
9.0	11.10.2018	DD	Freigabe
10.00	16.10.2018	ME	Freigabe
11.00	17.07.2019	ME	Freigabe
12.00	27.02.2020	HH	Freigabe
13.00	04.06.2020	HH	Freigabe
14.00	16.09.2020	Telekom Security	Freigabe
15.00	12.02.2021	Telekom Security	Freigabe
15.01	17.02.2021	Telekom Security	Kapitel 3.2, 3.2.2.4.6, 3.2.2.4.18, 3.2.2.5.1, 3.2.5, 4.3.1, 4.6.3, 4.7.3, 4.7.11, 4.7.12, 9.6.3 und 9.6.4 aktualisiert.

15.02	10.03.2021	Telekom Security	Aktualisierung von Kapitel 5.2.1
15.03	11.03.2021	Telekom Security	Strukturelle Überarbeitung des Dokuments vorgenommen. Änderungen in Kap. 1.2, 5, 5.1, 5.1.1 bis 5.1.7, 5.2.2 bis 5.2.4, 5.5.1, 6.7, 7.1.6.3, 7.2.0, 7.2.2.3, 7.2.2.4, 12
15.04	08.04.2021	Telekom Security	Änderungen in Kap. 4.2.2, 4.9.1.2, 6.6.2
15.05	23.04.2021	Telekom Security	Änderungen in Kap. 1.5.2, 4.9.7, 4.9.12, 4.10.2, 6.1.5, 6.1.6, 7.1.3, 7.1.3.1, 7.1.3.2. Impressum geändert. Tabellen überarbeitet.
15.06	28.04.2021	Telekom Security	Änderungen in Kap. 3.2.2.4.18, 4.9.5, 9.2.1, 12
16.00	29.04.2021	Telekom Security	Freigabe

Hinweis: Für die vollständige Nachvollziehbarkeit der Änderungen ist die Vorgängerversion zu verwenden.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 EINLEITUNG

Die Deutsche Telekom AG betreibt seit 1994 ein Trust Center (Telekom Trust Center), das 1998 als erstes Trust Center bundesweit die Genehmigung zur Ausgabe von Zertifikaten für die digitale Signatur gemäß dem damaligen Deutschen Signaturgesetz erhielt.

Das Telekom Trust Center wurde durch die Konzerneinheit T-Systems International GmbH betrieben und ist seit 1996 nach ISO 9002 und seit Januar 2001 nach ISO 9001:2000 zertifiziert.

Der Betrieb ging im Rahmen einer Abspaltung ab dem 01.07.2020 auf die Deutsche Telekom Security GmbH (im Folgenden „DT Security GmbH“) über.

Zusätzlich zu den genau festgelegten und zertifizierten Arbeitsabläufen zeichnet sich das Trust Center durch einen sehr hohen Sicherheitsstandard aus. Die Vertrauenswürdigkeit des eingesetzten Trust Center Personals ist durch öffentliche Stellen überprüft worden. Alle Dienste sind Gegenstand regelmäßiger Qualitätskontrollen. Die eingesetzte Technologie ist Stand der Technik und wird laufend durch ausgebildete Administratoren überwacht.

Das Trust Center betreibt eine Reihe unterschiedlicher Zertifizierungsstellen unter verschiedenen Wurzel-Instanzen (Roots) für unterschiedliche elektronische Zertifikate. Die Zertifizierungsstellen der Zertifikats-Dienstleistungen unterscheiden sich hinsichtlich der Anwendungskontexte für Zertifikate, der konkreten Ausprägung der technischen Schnittstellen, Registrierungsverfahren, der Zertifikatsprofile, der Prozesse bei Sperrungen, sowie der Veröffentlichung von Informationen.

1.1 Überblick

TeleSec ServerPass ist eine im Trust Center betriebene PKI-Dienstleistung zur Ausstellung von verschiedenen X.509v3 Server-Zertifikaten. Der in Kapitel 1.5.1 genannte Bereich ist verantwortlich dafür, dass die beschriebenen Abläufe, Tätigkeiten, Systeme, Rollen und Sicherheitsmaßnahmen auch für den Fall durchgesetzt werden, wenn diese ausgelagert werden.

Der TeleSec ServerPass (SSL/TLS-Zertifikat) macht einen Internet-/Intranetserver identifizierbar und bindet die Identität der Organisation daran.

TeleSec ServerPass setzt sich zusammen aus den geprüften Angaben des Zertifikatsinhabers, dem öffentlichen Schlüssel des Webservers, Daten zum Aussteller des Zertifikates sowie der Signatur der Trust Center Zertifizierungsstelle. Durch die Möglichkeit der Verschlüsselung (SSL/TLS) wird zusätzlich für die Sicherheit der Kommunikation gesorgt. Die Verschlüsselungsstärke richtet sich nach den Möglichkeiten des Servers und der Endbenutzersoftware (Browser).

TeleSec ServerPass wird in verschiedenen Produktausprägungen angeboten.

ServerPass Zertifikate dienen dabei primär den folgenden Zwecken:

- Identifizierung der juristischen Person (Organisation), welche eine Webseite unter ihrer Kontrolle hat.
- Verschlüsselte Kommunikation mit einer Webseite.

1.1.1 TeleSec ServerPass Standard:

Das Standard Server Zertifikat erfüllt die obenstehenden Leistungsmerkmale und enthält genau einen FQDN, Hostname oder eine IP-Adresse, die von einem öffentlichen DNS aufgelöst werden kann.

1.1.2 TeleSec ServerPass SAN/UCC:

ServerPass SAN/UCC erfüllt ebenfalls die obenstehenden Leistungsmerkmale und bietet gegenüber ServerPass Standard die Möglichkeit zusätzlich weitere SAN-Felder zu belegen und setzt sich zusammen aus:

- Grundpaket (6-Pack): ein (1) öffentlicher FQDN (vollständiger Domainname) oder eine (1) öffentliche IP-Adresse und bis zu 5 Subdomains der öffentlichen Domain oder 5 Multi-Level-Subdomains der öffentlichen Domain
- weitere öffentliche FQDN oder weitere öffentliche IP-Adressen
- weitere Subdomains der öffentlichen Domains

1.1.3 TeleSec ServerPass EV:

Die Produktvariante TeleSec ServerPass EV (Extended Validation) erfüllt die obenstehenden allgemeinen Leistungsmerkmale und enthält genau einen FQDN (Hostname), der von einem öffentlichen DNS aufgelöst werden kann. Darüber hinaus bietet es zusätzliche Sicherheit unter anderem durch strengere Vergaberichtlinien nach [CABF-BREV] (siehe Kapitel 10.2) und einen erhöhten Aufwand im Registrierungsprozess.

1.1.4 TeleSec ServerPass EV SAN:

ServerPass EV SAN erfüllt die obenstehenden allgemeinen Leistungsmerkmale und bietet gegenüber ServerPass EV die Möglichkeit zusätzlich weitere SAN-Felder zu belegen und setzt sich zusammen aus:

- Grundpaket (5-Pack): ein (1) öffentlicher FQDN (vollständiger Domainname) und bis zu 4 Subdomains der öffentlichen Domain oder 4 Multi-Level-Subdomains der öffentlichen Domain
- weitere öffentliche FQDN
- weitere Subdomains der öffentlichen Domains

Weitere Zwecke von ServerPass EV sind:

- Erschweren von Phishing und betrügerischen Aktivitäten im Zusammenhang mit TLS/SSL-Zertifikaten.
- Unterstützung von Organisationen ihren Webseiten/Webservern eine eindeutige Identität zu geben.
- Die Strafverfolgungsbehörden bei ihrer Untersuchung von Phishing- und weiterem Online-Betrugsfällen unterstützen, inklusive, falls angemessen, Kontaktaufnahme, Untersuchen oder gerichtlich gegen das Subjekt vorgehen.

1.1.5 eIDAS:

Alle EV-Varianten erfüllen die eIDAS Anforderungen für EU qualifizierte Zertifikate und die ETSI EN 319 411-2 policy für QCP-w. ServerPass EV erfüllt die Anforderungen an qualifizierte Vertrauensdiensteanbieter (TSP) bzw. qualifizierte Vertrauensdienste für Website-Authentisierung gemäß eIDAS-Verordnung (EU) No 910/2014.

Webseiten, die Extended Validation Zertifikate einsetzen, werden in aktuellen Browsern farblich hervorgehoben. Dies kann, je nach verwendetem Webbrowser durch eine grün hinterlegte Adressleiste, durch eine grüne Schriftfarbe im Adressfeld oder ähnlich erfolgen. Es können zusätzliche Informationen über die Validierung angezeigt werden. Für den Nutzer wird der höhere Registrierungs- und Validierungsaufwand somit optisch auffällig markiert.

Bei der Registrierung aller ServerPass Varianten werden die folgenden Sachverhalte ausdrücklich **nicht** geprüft:

- Dass die im Zertifikat genannte Organisation einer aktiven Geschäftstätigkeit nachgeht.
- Dass die im Zertifikat genannte Organisation in ihrer Geschäftstätigkeit gesetzeskonform handelt.
- Dass die im Zertifikat genannte Organisation in ihrer Geschäftstätigkeit vertrauenswürdig, ehrlich oder seriös handelt.
- Dass es ungefährlich bzw. sicher ist, mit der im Zertifikat genannten Organisation Geschäfte zu tätigen.

Ergänzend zu den Allgemeinen Geschäftsbedingungen TeleSec-ServerPass [AGB] werden die Verfahrensweisen zur Ausstellung und Verwaltung von TeleSec ServerPass im Rahmen der zertifikatsbasierten Public Key Infrastruktur (PKI) beschrieben.

Das CPS ermöglicht aufgrund der vorliegenden Beschreibungen die qualitative Einschätzung der Dienstleistung.

Das vorliegende Dokument orientiert sich an dem internationalen Standard für Zertifizierungsrichtlinien und Erklärungen zum Zertifizierungsbetrieb, dem „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“ [RFC3647] der Internet Society (ISOC).

In einigen Kapiteln wird Bezug auf die durch die EV SSL Certificate Guidelines [CABF-BREV] gesetzten Richtlinien des CA/Browser Forums genommen.

Darüber hinaus entsprechen die ServerPass EV Zertifikate dem ETSI Standard für Web Zertifikate [ETSI WEB].

1.1.6 Einhaltung der Baseline Requirements des CA/Browser Forums

Das Trust Center sichert zu, dass die für TeleSec ServerPass verwendeten Sub-CAs die Anforderungen und Regelungen der jeweils aktuellen veröffentlichten Version der [CABF-BR] https://cabforum.org/baseline-requirements/ und der [CABF-BREV] https://cabforum.org/extended-validation/ erfüllt und einhält. Im Falle eines Widerspruchs zwischen dem vorliegenden Dokument und den [CABF-BR], haben die Regelungen aus den [CABF-BR] Vorrang.

1.1.7 Einhaltung der übergreifenden Zertifizierungsrichtline des Trust Centers

Das Trust Center sichert zu, dass für TeleSec ServerPass die Anforderungen der übergreifenden Zertifizierungsrichtline des Trust Centers der Telekom Security ("Telekom Security CP" mit der OID 1.3.6.1.4.1.7879.13.42) umgesetzt sind bzw. eingehalten werden. Die Telekom Security CP ist im Internet veröffentlicht unter https://www.telesec.de/de/service/downloads/pki-repository/.

1.2 Dokumentenidentifikation

Dieses Dokument trägt den Namen „CPS TeleSec ServerPass“.

Die verbindlichen Angaben zu Version, Gültigkeitsdatum und Status sind auf dem Deckblatt aufgeführt.

1.3 PKI-Beteiligte

Im Folgenden wird explizit auf die PKI-Beteiligten des Dienstes TeleSec ServerPass eingegangen.

1.3.1 Zertifizierungsstellen

Die Zertifizierungsstelle (CA Certification Authority) ist der Teil einer Public Key Infrastruktur, der Zertifikate ausstellt, verteilt und Prüfmöglichkeiten zur Verfügung stellt. Für TeleSec ServerPass stehen, je nach Produktvariante oder Anforderung, unterschiedliche Stammzertifizierungsstellen (Root-CAs) zur Verfügung. Anforderungen an die Root-CAs sowie an die von der Root-CA ausgestellten Sub-CA-Zertifikate sind im CP der jeweiligen Root-CA nachzulesen.

Sub-CAs, die nicht mehr produktiv Endteilnehmer-Zertifikate ausstellen, werden noch für die Signatur von Sperrlisten und/oder OCSP-Antworten verwendet, solange es erforderlich ist.

Die Zertifizierungsstelle stellt Stammzertifizierungsstelle(n) (Root-CA) je Produktvariante zur Verfügung. Je nach Produktausprägung können Root-CA und/oder Sub-CA variieren. Neue Vertrauensanker und Sub-CAs können angeboten oder Bestehende vom Markt genommen werden. Grund dafür sind sich ändernde nationale und/oder internationale Anforderungen, neue Sicherheitsverfahren, Kompromittierung bestehender Sicherheitsverfahren oder andere Gründe. Daraus resultierende Aufwände, die sich möglicherweise auf Kundenseite ergeben, gehen nicht zu Lasten der Zertifizierungsstelle.

Die aktuell verwendeten Root-Zertifikate bieten große Marktdurchdringung, Kompatibilität und Flexibilität. Sicherheitshinweise lassen sich durch die Installation des Zwischenstellen-Zertifikat vermeiden, sodass der Endteilnehmer während des Verbindungsaufbaus durch keinerlei interpretationswürdige Sicherheitshinweise irritiert wird. Eine Übersicht aller verwendeten Zertifizierungsstellen ist in Kapitel 7.1.2.9 zu finden.

Alle Komponenten unterliegen ununterbrochen seit 2008 den für die Ausstellung erforderlichen jährlichen Zertifizierungen.

Alle TeleSec ServerPass Sub-CAs stellen ausschließlich Endteilnehmer-Zertifikate aus und werden für die Signatur von Sperrlisten und/oder OCSP-Antworten verwendet. Insbesondere werden keine Sub-CA-Zertifikate ausgestellt. Sowohl die Stammzertifizierungsstellen (Root-CAs) als auch die Zwischenzertifizierungsstellen (Sub-CAs) können aufgrund von sich ändernden technischen oder sonstigen Anforderungen variieren. Das Validierungsmodell basiert auf dem Schalenmodell, d.h. jedes Zertifikat ist maximal so lange gültig, wie das darüber liegende ausstellende Zertifikat gültig ist.

Mit TeleSec ServerPass bietet DT Security GmbH eine PKI-Lösung an, dessen Infrastruktur im einem Trust Center installiert ist und von qualifiziertem Personal betrieben wird. Alle sicherheitsrelevanten Aktionen erfolgen über eine verschlüsselte Verbindung (HTTPS).

Für TeleSec ServerPass stehen verschiedene Stammzertifizierungsstellen (Root-CAs) zur Verfügung. Diese können während der Beauftragung ausgewählt werden. Eine Übersicht der Zertifizierungsstellen ist in den nachfolgenden Abbildungen dargestellt. Der Geltungsbereich dieses Dokuments umfasst die in den rot gestrichelten Bereichen enthaltenen Sub-CA’s und Zertifikate aus diesen Abbildungen.

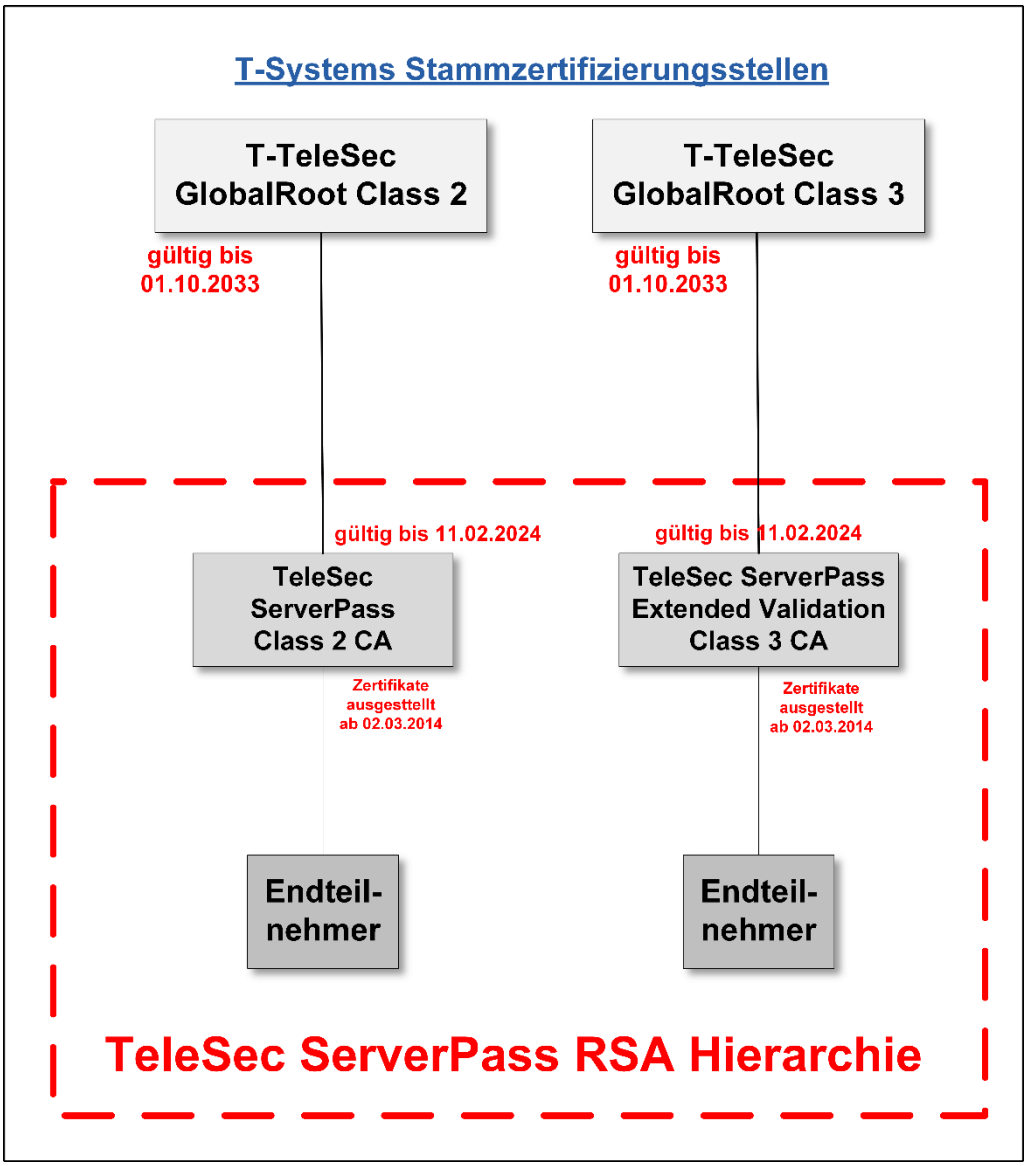

Abbildung 1: Übersicht der RSA-Zertifikatshierarchien für TeleSec ServerPass

Sowohl die Stammzertifizierungsstelle (Class 3 Root-CAs), als auch deren untergeordnete Zertifizierungsstelle (Sub-CA) werden konform zu den jeweils aktuell gültigen Richtlinien zur Ausgabe und Verwaltung von Extended Validation Zertifikaten („Richtlinien“), welche unter http://www.cabforum.org veröffentlich sind, betrieben. Sollte dieses Dokument und die Richtlinien voneinander abweichen, so gelten die Richtlinien vorrangig.

1.3.2 Registrierungsstellen

Eine Registrierungsstelle (RA) ist eine Stelle, die die Identifizierung und Authentifizierung von Auftraggebern durchführt, Zertifikatsaufträge bearbeitet (genehmigt, ablehnt, Wiedervorlage), Sperraufträge bearbeitet oder weiterleitet.

Grundsätzlich muss eine Registrierungsstelle (RA) gewährleisten, dass keine unberechtigte Person oder Maschine in den Besitz eines Zertifikats gelangt.

Die Trust Center Registrierungsstelle hat insbesondere folgende Aufgaben:

- Entgegennahme von Aufträgen und Prüfung der Identifikationsunterlagen,
- Prüfen der Dokumente auf Echtheit und Vollständigkeit,
- Identifikation der juristischen Person (siehe Kapitel 3.2),

  - Organisationsprüfung
  - Identitätsprüfung
  - Domain-Prüfung
  - Autorisierungsprüfung
- Genehmigung der Zertifikatsausstellung,
- Sperren von Zertifikaten, wenn Sperrgründe vorliegen (siehe Kapitel 4.9).

Zur Registrierung von TeleSec ServerPass Zertifikaten sind keine Registrierungsstellen Dritter (externe RA) zugelassen.

TeleSec ServerPass EV/EV SAN:

Bei der Produktvariante TeleSec ServerPass EV/EV SAN arbeitet die Registrierungsstelle bei der Durchführung der oben genannten Aufgaben streng gemäß der EV-Richtlinien des CA/Browser Forums [CABF-BREV].

1.3.3 Endteilnehmer (End Entity)

Unter Endteilnehmer werden alle Zertifikatsnutzer verstanden, auf die ein Zertifikat ausgestellt werden kann.

Es werden nur Zertifikate an juristische Personen (z.B. Stiftungen bürgerlichen Rechts, Körperschaften des Privatrechts wie Aktien Gesellschaften, eingetragene Vereine, Gesellschaften mit beschränkter Haftung, eingetragene Genossenschaften) ausgestellt.

1.3.4 Vertrauender Dritter

Ein vertrauender Dritter (Relying Party) ist eine natürliche Person oder Subjekt, die/das sich auf die Vertrauenswürdigkeit des von der Zertifizierungsstelle ausgestellten Zertifikats und/oder digitalen Signatur verlässt.

Unter Vertrauende Dritte werden beispielsweise auch Software-Hersteller verstanden, die Root- und Sub-CA-Zertifikate von TeleSec ServerPass in die Zertifikatsspeicher integrieren.

1.3.5 Andere Teilnehmer

Für TeleSec ServerPass werden keine Funktionen und/oder Aufgaben an externe Stellen ausgelagert (Delegated Third Party), welche den Betrieb der CA-Infrastruktur, die Prüfung, Genehmigung, Bearbeitung oder Verwaltung von Zertifikaten oder Zertifikatsaufträgen betreffen.

1.4 Zertifikatsverwendung

1.4.1 Zulässige Verwendung von Zertifikaten

TeleSec ServerPass Zertifikate dürfen nur im zulässigen und geltenden gesetzlichen Rahmen verwendet werden. Dies gilt insbesondere unter Beachtung der länderspezifischen geltenden Ausfuhr- und Einfuhrbestimmungen.

Die Zertifizierungsstelle stellt nur Zertifikate für juristische Personen aus.

Verwendungszweck TLS/SSL Zertifikate

Tabelle 2: Verwendung von Zertifikaten für juristische Personen

	Verschlüsselung	Authentisierung	Sichere online Kommunikation	Prüfniveau
TeleSec ServerPass Standard	Ja	Ja	Ja	medium
TeleSec ServerPass SAN/UCC	Ja	Ja	Ja	medium
TeleSec ServerPass EV/EV SAN (Extended Validation)	Ja	Ja	Ja	hoch

1.4.2 Unzulässige Verwendung von Zertifikaten

TeleSec ServerPass und TeleSec ServerPass-EV-Zertifikate sind nicht zur Verwendung oder zur Weitergabe vorgesehen, ausgelegt oder zugelassen für

- Steuerungs- und Kontrolleinrichtungen in gefährlichen Umgebungen,
- Umgebungen in denen ein ausfallsicherer Betrieb gefordert ist (z.B. der Betrieb von nuklearen Einrichtungen, Flugzeugnavigations- oder -kommunikationssystemen, Luftverkehrs-Kontrollsystemen oder Waffenkontrollsystemen), wobei ein Ausfall zu Schäden (z.B. Personenschäden, Tod, mittleren und schweren Umweltschäden, sonstige Katastrophen) führen kann.

Endteilnehmer-Zertifikate dürfen nur für den zugelassenen Verwendungszweck und nicht als Zertifizierungsstelle (Sub-CA) oder Stammzertifizierungsstelle (Root-CA) eingesetzt werden.

1.5 Verwaltung des Dokuments

1.5.1 Zuständigkeit für das Dokument

Dieses Dokument wird von

Deutsche Telekom Security GmbH
Trust Center & ID Solutions, Chapter Trust Center Products
Untere Industriestraße 20
57250 Netphen

herausgegeben.

1.5.2 Kontaktinformationen

Deutsche Telekom Security GmbH
Trust Center & ID Solutions, Chapter Trust Center Products
Untere Industriestraße 20
57250 Netphen
Deutschland

Telefon: +49 (0) 1805 268 204 (Festnetz 0,14 EUR/Minute, Mobilfunknetze max. 0,42 EUR/Minute)
E-Mail: telesec_support@t-systems.com
Internet: https://www.telesec.de

Für allgemeine Anfragen verwenden Sie bitte den folgenden Eingangskanal:

https://www.telesec.de/de/service/kontakt/anfragemitteilung/.

Zertifikatsmissbräuche, Schlüsselkompromittierungen, fehlerhafte bzw. nicht-konforme Zertifikate, andere sicherheitsrelevante Zertifikatsprobleme oder der Verdacht auf solche Vorfälle können unter

https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden/

oder via FMB_Trust_Center_Rootprogram@t-systems.com

an Telekom Security gemeldet werden. Dabei sollten möglichst viele Informationen enthalten sein, die eine Verifizierung des Problems möglich machen. Im Falle einer Kompromittierung sollte dies bspw. einen mit dem privaten Schlüssel signierten CSR mit commonName „Compromised Key“ beinhalten.

Telekom Security wird ggf. Strafverfolgungsbehörden und Aufsichtsbehörden einschalten. Die Eingabe der Meldung wird als Einverständnis gewertet, dass Daten ohne weitere Einwilligung in einem solchen Fall an Behörden weitergegeben werden können.

1.5.3 Stelle, die über die Vereinbarkeit dieser Richtlinien mit der CP entscheidet

In Kapitel 1.5.1 ist die Organisation aufgeführt, die sich verantwortlich zeigt, dass diese CPS oder Dokumente, die dieses Dokument ergänzen oder untergeordnet sind, mit der Zertifizierungsrichtlinie (Certificate Policy, CP) vereinbar sind.

1.5.4 Genehmigungsverfahren dieses Dokuments

Die Genehmigung erfolgt durch einen formalen Dokumentenfreigabeprozess.

Dieses Dokument behält Gültigkeit, solange es nicht vom Herausgeber (siehe Kapitel 1.5.1) widerrufen wird. Es wird bei Bedarf fortgeschrieben, und erhält dann jeweils eine neue aufsteigende Versionsnummer (siehe auch Kapitel 9.12.1 und 9.12.2).

1.6 Akronyme und Definitionen

Akronyme und Begriffsdefinitionen finden Sie in Kapitel 12**.**

2 VERANTWORTLICHKEITEN FÜR VERÖFFENTLICHUNGEN UND ABLAGEN

2.1 Ablagen

Das Trust Center betreibt für die Dienstleistung TeleSec ServerPass einen Verzeichnisdienst und eine zentrale Datenablage und ist für die Inhalte verantwortlich.

Extrakte dieser Datenbanken stellen in aufbereiteter Form die Basis dar, um Zertifikatsinformationen und Zertifikatssperrliste (CRL) auf dem Verzeichnisdienst zu veröffentlichen oder den Validierungsdienst (OCSP-Responder) mit Statusinformationen zu versorgen.

Weiterhin werden für die Öffentlichkeit relevante Dokumente in Form einer zentralen Datenablage (Repository) zur Verfügung gestellt. Diese umfasst insbesondere die entsprechenden Dokumente der beteiligten Zertifizierungsstellen (Root- und Sub-CAs). Dieses Verzeichnis ist 7x24 Stunden verfügbar. Die Ausfallzeit beträgt maximal 1,5 Tage im monatlichen Mittel.

Das Trust Center setzt geeignete Mechanismen zum Schutz der zentralen Datenablage (Repository) gegen nicht autorisierte Manipulationsversuche (hinzufügen, löschen, ändern) ein.

2.2 Veröffentlichung von Zertifikatsinformationen

Die Zertifizierungsstelle veröffentlicht in regelmäßigen Abständen Zertifikatssperrlisten (CRL). Die Zertifikatssperrlisten enthalten Zertifikate, die von einer TeleSec ServerPass CA ausgestellt und vor dem Erreichen des Ablaufdatums gesperrt wurden. Es werden nur Zertifikate gesperrt, die zum Sperrzeitpunkt gültig sind.

Ferner steht der Validierungsdienst (OCSP-Responder) zur Verfügung, der über das Internetprotokoll „Online Certificate Status Protocol“ (OCSP) erreichbar ist und den Status von X.509-Zertifikaten zurück liefert.

Die aktuellsten ServerPass-Dokumente werden hier veröffentlicht:

https://www.telesec.de/de/service/downloads/pki-repository/

Erläuterung zur Menü-Struktur:

- Das ServerPass CPS befindet sich im Menü „Certificate Practice Statement (CPS) -> ServerPass“
- Das ServerPass PDS befindet sich im Menü „PKI Disclosure Statement (PDS)“
- Die Root-CA-Zertifikate befinden sich im Menü „Root-CA Certificates“
- Die ServerPass Sub-CA-Zertifikate befinden sich im Menü „Sub-CA Certificates -> ServerPass“

Server-Zertifikate, die einen CT-Log-Eintrag enthalten (Kapitel 4.4.2), werden über Log-Server von Dritten (z.B. Google) veröffentlicht.

Zusätzlich werden Testseiten betrieben (z.B. für Software-Entwickler), die Auskunft über den Status (gültig, gesperrt und abgelaufen) eines Webserver-Zertifikats in Abhängigkeit von der Stamm-Zertifizierungsstelle (Root-CA) anzeigt.

Es werden die folgenden Testseiten betrieben:

https://root-class2.test.telesec.de

https://root-class2-revoked.test.telesec.de

https://root-class2-expired.test.telesec.de

https://root-class3.test.telesec.de

https://root-class3-revoked.test.telesec.de

https://root-class3-expired.test.telesec.de

Die oben genannten Informationen werden auf der Webseite https://www.telesec.de/, Reiter „Root Programm > Informationen zu CA-Zertifikaten > Root-CA-Zertifikate“ veröffentlicht. Zusätzlich erfolgt bei sicherheitskritischen Vorfällen eine Benachrichtigung der Zertifikatsinhaber in schriftlicher Form, im Internet oder per E-Mail.

Änderungen der Informationssicherheitspolitik werden den Bewertungsstellen/Auditoren (Kapitel 8 ff.) und/oder der Aufsichtsbehörde mitgeteilt.

Die Zertifizierungsstelle bietet über den Link https://www.telesec.de/de/root-programm/support/pki-service-ermitteln/ eine Umkehrsuche an. Nach dem Hochladen eines Endteilnehmer-Zertifikats (binär oder base64-kodiert) werden folgende Informationen angezeigt:

- Aussteller (Issuer-DN)
- Antragsteller (Subject-DN)
- Zertifikatsseriennummer
- Gültigkeitsbeginn
- Gültigkeitsende
- Länge des öffentlichen Schlüssels (Bit)
- Signaturalgorithmus
- Link zur Erklärung zum Zertifizierungsbetrieb (CPS)
- Link zu den ServerPass Leistungen und Nutzungsbedingungen
- Link zu den Allgemeinen Geschäftsbedingungen TeleSec-ServerPass [AGB]
- Link zu den Nutzungsbedingungen
- Link zum PKI Disclosure Statement
- Link zu den CA-Zertifikaten

Hinweis: Die Umkehrsuche wird derzeit nur von den Browsern (Vollversionen) Microsoft Edge, Mozilla Firefox und Google Chrome unterstützt.

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

Aktualisierungen des CPS werden wie in Kapitel 9.12 beschrieben veröffentlicht.

Das vorliegende CPS wird unabhängig von weiteren Änderungen einer jährlichen Überprüfung (Review) unterzogen. Verantwortlich für die Durchführung bzw. die Koordination des Reviews ist die in Kapitel 1.5.1 benannte Stelle.

Das jährliche Review wird in der Änderungshistorie des CPS zu vermerkt. Dies gilt auch für den Fall, dass keine inhaltlichen Änderungen vorgenommen werden. Aktuelle Entwicklungen,

Änderungen und geänderte Anforderungen (zum Beispiel durch CABF-BR) werden verfolgt und in der Releaseplanung berücksichtigt.

Die Zertifikatssperrliste und die OCSP-Antworten werden wie in Kapitel 4.9.7 beschrieben veröffentlicht.

2.4 Zugang zu den Ablagen und Informationsdiensten

Der Abruf der Sperrlisten (CRL, ARL) und der OCSP-Service unterliegt für Endteilnehmer (Kapitel 1.3.3) oder Vertrauende Dritte (Kapitel 1.3.4) keiner Zugriffskontrolle. Der Lesezugriff auf diese Informationen unterliegt keiner Beschränkung.

Die Integrität und Authentizität der Sperrlisten und OCSP-Auskünfte wird durch die digitale Signatur mit vertrauenswürdigen Signern gewährleistet (Kapitel 4.10.1).

Der lesende Zugriff für die Zertifikatsnehmer und -nutzer auf Informationen der CA- und Root-CA (siehe Kapitel 2.2) über einschlägige Webseiten unterliegt ebenfalls keiner Zugriffskontrolle. Dies gilt ebenfalls für das Verzeichnis des veröffentlichten CPS.

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Namensregeln

Ein Distinguished Name (DN) ist ein globaler, eindeutiger Name für Verzeichnisobjekte nach dem X.500 Standard. Mit dem Distinguished Name ist eine weltweite eindeutige Unterscheidbarkeit von Personen und Systemen gegeben. Der DN stellt sicher, dass nie ein digitales Zertifikat für verschiedene Personen mit dem gleichen Namen ausgestellt wird.

Innerhalb eines Zertifikates ist zu unterscheiden nach

- IssuerDistinguishedName (Issuer DN)
- SubjectDistinguishedName (Subject DN)

Alle Subject-Angaben müssen durchgängig in einer Sprache - entweder in Deutsch oder der englischen Übersetzung - eingetragen werden.

3.1.1 Namensformen

Für alle auszustellenden SSL/TLS-Zertifikate wird die Identität des Zertifikatnehmers geprüft. Die entsprechenden Informationen werden in das Zertifikat übernommen.

Es müssen zumindest die folgenden Pflichtfelder ausgefüllt sein:

- organizationName O (Organisation)
- localityName L (Stadt)
- countryName C (Staat)
- stateOrProvinceName ST (Bundesland/Region/Provinz) (nur EV/EV SAN)

Die oben genannten Felder durchlaufen eine Datenbank gestützte Konsistenzprüfung. Abweichungen werden deutlich angezeigt. Um die Korrektur dieser Abweichungen ohne neue Requesterzeugung zu ermöglichen, können diese Felder durch den Auftraggeber manuell geändert werden. Das mit diesen geänderten Feldern ausgestellte Zertifikat entspricht dann aber nicht mehr den Daten des ursprünglichen Requests. Es kann Applikationen und Konstellationen geben (z.B. Microsoft IIS) bei denen es zu Problemen bei der Installation (Import) des Zertifikats kommt. Es empfiehlt sich deshalb, anstatt der Korrektur, einen neuen Zertifikatsrequest für diese Beauftragung zu verwenden.

Es werden keine DomainValidation-Zertifikate (DV) ausgestellt.

Mit der Ausnahme des Feldes subject:organizationalUnitName (OU) werden ausschließlich Informationen in ein Feld des Subject eingetragen werden, welche auf Korrektheit (Richtigkeit und Vollständigkeit) überprüft wurde.

Die Verwendung von "Metazeichen", wie z.B. "-", "." oder " " (Space) zur Signalisierung, dass ein Feld nicht mit Informationen des Zertifikatnehmers belegt oder nicht relevant (n/a) ist, ist nicht erlaubt.

3.1.1.1 TeleSec ServerPass Standard und SAN/UCC: Konventionen für Namensbestandteile

Im Folgenden werden zum Teil die englischen Begriffe verwendet, die auch in Deutschland inzwischen gebräuchlich sind.

3.1.1.1.1 SubjectAlternativeName (Pflichtfeld)

Die Erweiterung SubjectAlternativeName muss mindestens einen Eintrag enthalten. Wenn der Zertifikatsrequest die Erweiterung SubjectAlternativeName nicht enthält, wird der CommonName von der Zertifizierungsstelle in das erste SAN-Feld eingetragen. Bei TeleSec ServerPass ist dies der SubjectCommonName. Bei dem Eintrag handelt es sich in der Regel entweder um einen DNS Namen in der Form des FQDN (Fully Qualified Domain Name) oder um eine öffentliche IP-Adresse.

Die Zertifizierungsstelle stellt ab dem 01. Juni 2013 kein Zertifikat mehr aus, das im Feld SubjectAlternativeName oder SubjectCommonName eine IP-Adresse/eine Top-Level-Domain aus einem reservierten Adressraum oder einen internen Server-/Hostnamen enthält.

SAN-Felder dürfen nur die folgenden Zeichen enthalten: A-Z, a-z, 0-9, . (Punkt), * (Sternchen), - (Bindestrich).

TeleSec ServerPass Standard, -SAN/UCC: Einträge, die den Platzhalter „*“ (Sternchen) als Wildcard enthalten sind erlaubt. Bestimmte Zusammensetzungen von Wildcard-Zeichen und Zeichen und/oder Buchstaben (z.B. h*l.example.com) sowie mehr als ein Wildcard-Zeichen (z.B. *.*.example.com) pro FQDN werden nicht akzeptiert.

Für den Subject DN werden die folgenden Konventionen festgelegt.

3.1.1.1.2 OrganizationName (O) (Pflichtfeld)

Dieses Feld enthält den Organisationsnamen (z.B. Firma, Institution, Behörde) des Zertifikatsinhabers. Der Organisationsname im Zertifikat soll die offizielle Schreibweise der Organisation aufweisen, also identisch mit dem jeweiligen Registereintrag (Handelsregister o.ä.) sein. Es kann auch die offizielle Abkürzung verwendet werden. Zudem kann von der offiziellen Schreibweise der Rechtsform abgewichen werden, wenn eine gebräuchliche Abkürzung verwendet wird. Die Rechtsform ist nicht verpflichtend anzugeben. Beispiel: O=Musterfirma Gesellschaft mit beschränkter Haftung, O=Musterfirma GmbH oder O=Musterfirma. Das Attribut „O“ darf nur einmal angegeben werden.

Die Zertifizierungsstelle prüft diese Angabe im Verlauf des Registrierungsprozesses anhand des Handelsregisterauszugs oder gleichwertiger, verlässlicher Verzeichnisse/Dokumente. Leichte Abweichungen der Schreibweise des Organisationsnamens können akzeptiert werden, solange der Organisationsname weiterhin eindeutig ist (O=Alpha-Firma AG oder O=Alpha Firma AG).

Die Zertifizierungsstelle wird den Antragsteller zur Korrektur auffordern oder die akzeptierte Abweichung vom offiziellen Firmennamen dokumentieren.

3.1.1.1.3 OrganizationalUnitName (OU) (optional)

Dieses Feld ist **optional** und enthält eine Organisation, Einheit (Abteilung, Bereich) bzw. Abteilung/Unterabteilung oder Gruppe, Team. Sollten OU-Felder genutzt werden, so ist darauf zu achten, dass eine Verbindung zur Organisation (O) hergestellt werden kann. Das Attribut „OU“ kann mehrfach angegeben werden.

Beispiel: OU1=Einkauf, OU2=Niederlassung Musterstadt

Falls Angaben in diesem Feld gemacht werden, so werden diese im Verlauf des Registrierungsprozesses verifiziert. Verwirrende, irreführende oder missverständliche Angaben sind nicht zulässig. Die Zertifizierungsstelle wird die Ausstellung des Zertifikats verweigern, wenn eine Prüfung nicht oder nur mit sehr hohem Aufwand möglich ist.

3.1.1.1.4 CommonName (CN) Pflichtangaben (optional)

Dieses Feld muss, wenn es vorhanden ist, einen einzelnen FQDN (Fully Qualified Domain Name), also den vollständigen Namen einer öffentlich auflösbaren Domain. oder eine einzelne öffentliche IP-Adresse eines subjectAltName extension Feldes enthalten.

Die Verwendung einer IP-Adresse/einer Top-Level-Domain aus einem reservierten Adressbereich, eines internen Server-/Hostnamen oder einer IP-Adresse aus einem reservierten Adressraum in der Erweiterung extensions:subjectAltName oder in Feld subject:commonName ist nicht zulässig.

Beispiel: CN=www.example.de

Der Common Name darf die folgenden Zeichen enthalten: A-Z, a-z, 0-9, . (Punkt), * (Sternchen), - (Bindestrich)

Das Wildcard-Zeichen (*, Sternchen, Asterisk) wird nur ganz links im FQDN akzeptiert. Wildcard-Zeichen in Verbindung mit Zeichen und/oder Buchstaben (z.B. h*l.example.com) sowie mehr als ein Wildcard-Zeichen (z.B. *.*.example.com) pro FQDN werden nicht akzeptiert.

3.1.1.1.5 LocalityName (L) (Pflichtfeld)

Dieses Feld enthält den Namen der Stadt, in dem die Organisation (z.B. Firma, Institution, Behörde) ansässig ist. Es muss der vollständige, offizielle Ortsname verwendet werden.

Falls der Ortsname mehrmals in einem Land existiert, muss die Eindeutigkeit zusätzlich durch:

- die Postleitzahl = postalCode,

- und/oder das Bundesland = StateOrProvinceName (ST)

sichergestellt werden.

Beispiel: L=Frankfurt am Main, L=Frankfurt (Oder)

Die Zertifizierungsstelle prüft diese Angabe als Bestandteil der Adresse im Verlauf des Registrierungsprozesses anhand des Handelsregisterauszugs „HR-Auszug“ oder gleichwertiger, verlässlicher Verzeichnisse/Dokumente. Akzeptabel ist auch ein prüfbarer Nachweis eines vom obigen Dokument abweichenden Standorts.

3.1.1.1.6 StateOrProvinceName (ST) (optional)

Dieses Feld enthält das Bundesland, in dem die Organisation (z.B. Firma, Institution, Behörde) ansässig ist. Es wird die Schreibweise der Bundesländer nach ISO 3166-2 (mit und ohne Ländercode) akzeptiert.

Für die Bundesländer Nordrhein-Westfalen (NRW) und Rheinland-Pfalz (RLP) kann auch die in Klammern angegebene gebräuchliche Abkürzung verwendet werden. Für die Bundesländer Bayern, Sachsen und Thüringen kann auch die Bezeichnung „Freistaat “ vorangestellt werden.

Beispiel: ST=NRW oder ST=Freistaat Bayern

Im Zuge des Registrierungsprozesses wird diese Angabe als Bestandteil der Adresse anhand des Handelsregisterauszugs „HR-Auszug“ oder gleichwertiger, verlässlicher Verzeichnisse/Dokumente geprüft. Akzeptabel ist auch ein prüfbarer Nachweis eines vom obigen Dokument abweichenden Standorts.

3.1.1.1.7 Country Name (C) (Pflichtfeld)

Dieses Pflicht-Attribut enthält die weltweite Landeskennung. Festgelegt ist ein aus zwei Großbuchstaben bestehender Code, welcher in ISO 3166-1, Alpha-2 (International Organization for Standardization) spezifiziert ist. Dieses Feld spezifiziert das Land, in welchem der Zertifikatsinhaber niedergelassen ist.

Beispiel: C=DE

Weitere Details finden Sie hier:

http://www.unece.org/cefact/locode/subdivisions.html

http://www.nationsonline.org/oneworld/country_code_list.htm

Im Zuge des Registrierungsprozesses wird diese Angabe als Bestandteil der Adresse anhand des Handelsregisterauszugs „HR-Auszug“ oder gleichwertiger, verlässlicher Verzeichnisse/Dokumente geprüft. Akzeptabel ist auch ein prüfbarer Nachweis eines vom obigen Dokument abweichenden Standorts.

3.1.1.1.8 StreetAddress (optional)

Dieses Feld enthält den Straßennamen, an dem die Organisation (z.B. Firma, Institution, Behörde) ansässig ist.

Beispiel: streetaddress=Hauptstraße 17

Im Zuge des Registrierungsprozesses wird diese Angabe als Bestandteil der Adresse anhand des Handelsregisterauszugs „HR-Auszug“ oder gleichwertiger, verlässlicher Verzeichnisse/Dokumente geprüft. Akzeptabel ist auch ein prüfbarer Nachweis eines vom obigen Dokument abweichenden Standorts.

3.1.1.1.9 PostalCode (optional)

Dieses Feld enthält die Postleitzahl der Stadt, in dem die Organisation (z.B. Firma, Institution, Behörde) ansässig ist.

Beispiel: postalcode=12345

Die Zertifizierungsstelle prüft diese Angabe als Bestandteil der Adresse im Verlauf des Registrierungsprozesses anhand des Handelsregisterauszugs „HR-Auszug“ oder gleichwertiger, verlässlicher Verzeichnisse/Dokumente. Akzeptabel ist auch ein prüfbarer Nachweis eines vom obigen Dokument abweichenden Standorts.

3.1.1.1.10 EmailAddress (E) (optional)

Daten aus dem Feld EmailAddress werden ignoriert und nicht in das Zertifikat übernommen.

3.1.1.2 TeleSec ServerPass EV/EV SAN: Konventionen für Namensbestandteile

3.1.1.2.1 SubjectAlternativeName (Pflichtfeld)

Die Erweiterung SubjectAlternativeName muss mindestens einen Eintrag enthalten. Wenn der Zertifikatsrequest die Erweiterung SubjectAlternativeName nicht enthält, wird der CommonName in das erste SAN-Feld eingetragen. Bei TeleSec ServerPass ist dies der SubjectCommonName. Bei dem Eintrag handelt es sich in der Regel entweder um einen DNS Namen in der Form des FQDN (Fully Qualified Domain Name).

SAN-Felder dürfen nur die folgenden Zeichen enthalten: A-Z, a-z, 0-9, . (Punkt), - (Bindestrich). Einträge, die den Platzhalter „*“ (Sternchen, Asterisk) als Wildcard enthalten, sind nicht erlaubt.

3.1.1.2.2 OrganizationName (O) (Pflichtfeld)

Dieses Feld enthält den Organisationsnamen (z.B. Firma, Institution, Behörde) des Zertifikatsinhabers. Der Organisationsname im Zertifikat soll die offizielle Schreibweise der Organisation aufweisen, also identisch mit dem jeweiligen Registereintrag (Handelsregister o.ä.) sein. Es kann auch die offizielle Abkürzung verwendet werden. Zudem kann von der offiziellen Schreibweise der Rechtsform abgewichen werden, wenn eine gebräuchliche Abkürzung verwendet wird. Die Rechtsform ist nicht verpflichtend anzugeben. Beispiel: O=Musterfirma Gesellschaft mit beschränkter Haftung, O=Musterfirma GmbH oder O=Musterfirma. Das Attribut „O“ darf nur einmal angegeben werden.

Die Zertifizierungsstelle prüft diese Angabe im Verlauf des Registrierungsprozesses anhand des Handelsregisterauszugs oder gleichwertiger, verlässlicher Verzeichnisse/Dokumente. Leichte Abweichungen der Schreibweise des Organisationsnamens können akzeptiert werden, solange der Organisationsname weiterhin eindeutig ist (O=Alpha-Firma AG, O=Alpha Firma AG).

Die Zertifizierungsstelle wird den Antragsteller zur Korrektur auffordern oder die akzeptierte Abweichung vom offiziellen Firmennamen dokumentieren.

3.1.1.2.3 OrganizationalUnitName (OU) (optional)

Dieses Feld enthält eine Organisation, Einheit (Abteilung, Bereich) bzw. Abteilung/Unterabteilung oder Gruppe, Team. Sollten OU-Felder genutzt werden, so ist darauf zu achten, dass eine Verbindung zur Organisation (O) hergestellt werden kann. Verwirrende oder missverständliche Angaben sind nicht zulässig.

Beispiel: OU1=Einkauf

Falls Angaben in diesem Feld gemacht werden, so werden diese im Verlauf des Registrierungsprozesses durch die Zertifizierungsstelle geprüft und verifiziert. Die Zertifizierungsstelle wird die Ausstellung des EV/EV SAN-Zertifikats verweigern, wenn eine Prüfung nicht oder nur mit sehr hohem Aufwand möglich ist.

3.1.1.2.4 CommonName (CN) (optional)

Dieses Feld muss, wenn es vorhanden ist einen einzelnen FQDN (Fully Qualified Domain Name), also den vollständigen Namen einer öffentlich auflösbaren Domain eines subjectAltName extension Feldes enthalten.

Die Verwendung von internen Servernamen oder IP-Adressen in der Erweiterung extensions:subjectAltName oder in Feld subject:commonName ist für EV/EV SAN-Zertifikate nicht zulässig.

Beispiel: CN=www.musterdomain.de

Einträge, die den Platzhalter „*“ (Sternchen, Asterisk) als Wildcard enthalten, sind nicht erlaubt.

Die Zertifizierungsstelle wird diese Angabe sowie die Besitzverhältnisse im Verlauf des Registrierungsprozesses anhand von öffentlich verfügbaren Verzeichnissen prüfen.

3.1.1.2.5 LocalityName (L) (Pflichtfeld)

Dieses Feld enthält den Namen der Stadt, in dem die Organisation ihren eingetragenen Geschäftssitz hat („Place of Business“). Es muss der vollständige, offizielle Ortsname verwendet werden. Abkürzungen, sowie sonstige Schreibweisen oder Zusätze sind nicht erlaubt.

Beispiel: L=Frankfurt am Main, L=Frankfurt (Oder)

Die Zertifizierungsstelle prüft diese Angabe als Bestandteil der Adresse im Verlauf des Registrierungsprozesses anhand des Handelsregisterauszugs „HR-Auszug“ oder gleichwertiger, verlässlicher Verzeichnisse/Dokumente. Akzeptabel ist auch ein prüfbarer Nachweis eines vom obigen Dokument abweichenden Standorts.

3.1.1.2.6 StateOrProvinceName (ST) (Pflichtfeld)

Dieses Feld enthält das Bundesland, in dem die Organisation ihren eingetragenen Geschäftssitz hat („Place of Business“). Es wird die Schreibweise der Bundesländer nach ISO 3166-2 (mit und ohne Ländercode) akzeptiert.

Für die Bundesländer Nordrhein-Westfalen (NRW) und Rheinland-Pfalz (RLP) kann auch die in Klammern angegebene gebräuchliche Abkürzung verwendet werden. Für die Bundesländer Bayern, Sachsen und Thüringen kann auch die Bezeichnung „Freistaat “ vorangestellt werden.

Beispiel: ST=Nordrhein-Westfalen

Die Zertifizierungsstelle prüft diese Angabe als Bestandteil der Adresse im Verlauf des Registrierungsprozesses anhand des Handelsregisterauszugs „HR-Auszug“ oder gleichwertiger, verlässlicher Verzeichnisse/Dokumente. Akzeptabel ist auch ein prüfbarer Nachweis eines vom obigen Dokument abweichenden Standorts.

3.1.1.2.7 CountryName (C) (Pflichtfeld)

Dieses Feld enthält die Landeskennung, in welchem der Zertifikatsinhaber seinen eingetragenen Geschäftssitz hat („Place of Business“). Dies ist ein aus zwei Großbuchstaben bestehender Code, welcher in ISO 3166-1, Alpha-2 (International Organization for Standardization) spezifiziert ist.

Beispiel: C=DE

Weitere Details finden Sie hier:

http://www.unece.org/cefact/locode/subdivisions.html

http://www.nationsonline.org/oneworld/country_code_list.htm

Die Zertifizierungsstelle prüft diese Angabe als Bestandteil der Adresse im Verlauf des Registrierungsprozesses anhand des Handelsregisterauszugs „HR-Auszug“ oder gleichwertiger, verlässlicher Verzeichnisse/Dokumente. Akzeptabel ist auch ein prüfbarer Nachweis eines vom obigen Dokument abweichenden Standorts.

3.1.1.2.8 StreetAddress (Street) (optional)

Dieses Feld ist **optional** und enthält den Straßennamen, an dem die Organisation ihren eingetragenen Geschäftssitz hat („Place of Business“).

Beispiel: streetaddress=Hauptstraße 17

Die Zertifizierungsstelle prüft diese Angabe als Bestandteil der Adresse im Verlauf des Registrierungsprozesses anhand des Handelsregisterauszugs „HR-Auszug“ oder gleichwertiger, verlässlicher Verzeichnisse/Dokumente. Akzeptabel ist auch ein prüfbarer Nachweis eines vom obigen Dokument abweichenden Standorts.

3.1.1.2.9 PostalCode (optional)

Dieses Feld ist **optional** und enthält die Postleitzahl der Stadt, in dem die Organisation ihren eingetragenen Geschäftssitz hat („Place of Business“).

Beispiel: postalcode=12345

Die Zertifizierungsstelle prüft diese Angabe als Bestandteil der Adresse im Verlauf des Registrierungsprozesses anhand des Handelsregisterauszugs „HR-Auszug“ oder gleichwertiger, verlässlicher Verzeichnisse/Dokumente. Akzeptabel ist auch ein prüfbarer Nachweis eines vom obigen Dokument abweichenden Standorts.

3.1.1.2.10 Business Category (Pflichtfeld)

Dieses **EV/EV SAN-spezifische** Feld gibt Auskunft über die Art der Gesellschaftsform. Der richtige Wert dieses Felds wird von der Zertifizierungsstelle in Abhängigkeit von der gesetzten Gesellschaftsform gesetzt.

Beispiel: businessCategory=Private Organization

Die Prüfung der Gesellschaftsform erfolgt seitens der Zertifizierungsstelle im Verlauf des Registrierungsprozesses.

3.1.1.2.11 Jurisdiction of Incorporation or Registration (Pflichtfelder)

Diese **EV/EV SAN-spezifischen** Felder (gemäß den unten genannten Abstufungen) geben Auskunft über die Adresse des zuständigen Amts- oder Registergerichts. Im Einzelnen handelt es sich um:

- jurisdictionOfIncorporationLocalityName,
- jurisdictionOfIncorporationStateOrProvinceName,
- jurisdictionOfIncorporationCountryName.

Diese Felder enthalten ausschließlich Informationen auf Ebene der registrierenden Stelle.

Zum Beispiel: Der Gerichtsstand für eine registrierende Stelle auf nationaler Ebene enthält Informationen über das Land, nicht aber über das Bundesland und die Stadt. Der Gerichtsstand für eine registrierende Stelle auf Bundeslandesebene enthält Informationen über das Land und über das Bundesland, nicht aber über die Stadt. Ein Registergericht auf Stadt-/Kreisebene würde alle drei Informationen enthalten. Im einfachsten Fall (Registergericht auf Landesebene) ist die Angabe der Landeskennung zwingend erforderlich.

Die Codierung des Landeskennzeichens ist ein aus zwei Buchstaben bestehender Code, welcher in ISO 3166-1, Alpha-2 (International Organization for Standardization) spezifiziert ist.

Beispiele:

- jurisdictionOfIncorporationLocalityName=Musterhausen
- jurisdictionOfIncorporationStateOrProvinceName=Musterbundesland
- jurisdictionOfIncorporationCountryName=ML (MusterLand)

3.1.1.2.12 Registration Number (Pflichtfeld)

Dieses **EV/EV SAN-spezifische** Feld enthält die eindeutige Registrierungsnummer. Für den Fall, das keine Registriernummer vergeben wird bzw. wurde, muss dieses Feld das Datum der Registrierung im Format nach ISO 8601: YYYY-MM-DD enthalten. Die Angabe im Feld Registration Number wird im Zertifikatssubjekt im Feld SERIALNUMBER hinterlegt.

Beispiele: SERIALNUMBER=HRB 3244

SERIALNUMBER=2005-10-23

3.1.1.2.13 EmailAddress (E) (optional)

Daten aus dem Feld EmailAddress werden ignoriert und nicht in das Zertifikat übernommen.

3.1.2 Aussagekraft von Namen

Endteilnehmer- und CA-Zertifikate müssen Namen im Subjekt des Zertifikats mit gebräuchlicher Wortbedeutung enthalten, anhand derer sich die Identität der Organisation feststellen lässt.

Der Name muss den Endteilnehmer bzw. die Organisation eindeutig und nachprüfbar identifizieren.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsinhaber

Nicht anwendbar. Zertifikate mit Pseudonymen oder anonyme Zertifikate werden nicht ausgestellt.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Nicht anwendbar.

3.1.5 Eindeutigkeit von Namen

Die Zertifizierungsstelle stellt sicher, dass Zertifikate für unterschiedliche Kunden aber mit gleichem Subject-DN durch die Vergabe einer Seriennummer im Subject-DN (siehe Kapitel 7.1.10) unterschieden werden.

Ein Kunde kann mehrere Zertifikate mit demselben eindeutigen Subject DN besitzen. Diese unterscheiden sich durch die Zertifikatsseriennummer.

3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen

Es liegt in der Verantwortung des Endkunden, dass die Namenswahl keine Warenzeichen, Markennamen, Markenrechte usw. oder Rechte des geistigen Eigentums verletzen. Die Zertifizierungsstelle TeleSec ServerPass ist nicht verpflichtet, solche Rechte zu überprüfen. Daraus resultierende Schadenersatzansprüche gehen zu Lasten des Endkunden.

3.2 Identitätsüberprüfungen bei Neubeauftragung

Die Neubeauftragung kann nur nach erfolgreicher Registrierung im Serviceportal <myServerPass> erfolgen.

Es werden nur die für die Verifizierung der Identität notwendigen Nachweise verlangt.

3.2.1 Methoden zum Besitznachweis des privaten Schlüssels

Der Auftraggeber muss bei einer Beauftragung gegenüber der Zertifizierungsstelle in geeigneter Weise nachweisen, dass er im Besitz des privaten Schlüssels ist, der dem zu zertifizierenden öffentlichen Schlüssel zugeordnet ist. Der Besitznachweis ist durch die Methode PKCS#10 erbracht.

3.2.2 Authentifizierung der Organisations- und Domainidentität

Alle Auftragsinformationen sind anhand mindestens einer der nachfolgenden Prüfungen zu verifizieren. Eine Liste mit Informationen zu den für die Erfüllung der EV-Verifikationsanforderungen verwendeten Registrierungsstellen ist im Online-Repository (https://www.telesec.de/de/service/downloads/pki-repository/) unter „Validation Resources“ veröffentlicht.

Für EV-Zertifikats-Aufträge mit QC-Statement (QWAC, QCP-w) gilt: Durch die Unterschrift des Vertreters des Auftraggebers bestätigt dieser die Verbindung zu dem oder den im Auftrag angegebenen FQDN.

3.2.2.1 Identität

Die Informationen zur Subjektidentität werden durch mindestens eine der folgenden Methoden verifiziert:

1. eine staatliche Stelle in dem Hoheitsgebiet der rechtmäßigen Gründung, Existenz oder Anerkennung des Auftraggebers (z. B. https://www.handelsregister.de bzw. https://handelsregister.ch),

2. eine Drittdatenbank, die regelmäßig aktualisiert und als zuverlässige Datenquelle betrachtet wird (Bisnode Deutschland GmbH: D&B Credit - https://credit.dnb.com/login),

3. einen Standortbesuch durch die CA oder eine Drittpartei, die als Agent für die CA tätig wird, oder

4. ein Bestätigungsschreiben.

3.2.2.2 Firmierung/Handelsname

Wenn die Informationen zur Subjektidentität eine Firmierung oder einen Handelsnamen enthalten, verifiziert die CA das Recht des Auftraggebers zur Nutzung der Firmierung/des Handelsnamens durch mindestens eine der folgenden Methoden verifizieren:

1. Dokumentation, die durch eine staatliche Stelle in dem Hoheitsgebiet der rechtmäßigen Gründung, Existenz oder Anerkennung des Auftraggebers vorgelegt oder durch die Kommunikation mit einer solchen Stelle belegt wird (z.B. https://www.handelsregister.de bzw. https://handelsregister.ch),

2. eine zuverlässige Datenquelle (Bisnode Deutschland GmbH: D&B Credit - https://credit.dnb.com/login),

3. Kommunikation mit einer staatlichen Stelle, die für die Verwaltung solcher Firmierungen oder Handelsnamen zuständig ist,

4. ein Bestätigungsschreiben, dem Nachweisdokumente beigefügt sind, oder

5. eine Rechnung eines Versorgungsunternehmens, eine Bankabrechnung, eine Kreditkartenabrechnung, ein vom Staat ausgegebenes Steuerdokument oder eine andere Form der Identifizierung, deren Zuverlässigkeit die CA feststellt.

3.2.2.3 Überprüfung der Länderkennung

Das zum Subjekt gehörende Land im Feld subject:countryName wird von der CA mithilfe einer der folgenden Methoden verifiziert werden:
1. die Zuweisung des IP-Adressenbereichs durch das Land für (i) die IP-Adresse der Webseite, wie durch den DNS-Eintrag für die Webseite angegeben, oder (ii) die IP-Adresse des Auftraggebers,
2. die ccTLD des beantragten Domain-Namens,
3. Informationen, die vom Domain-Name-Registrar vorgelegt werden, oder
4. eine in Abschnitt 3.2.2.1 identifizierte Methode.

3.2.2.4 Überprüfung der Berechtigung oder der Kontrolle der Domain

Für jeden vollqualifizierten Domain-Namen (FQDN), bestätigt die Zertifizierungsstelle, dass der Auftraggeber (oder die Muttergesellschaft, die Tochtergesellschaft oder das verbundene Unternehmen des Auftraggebers, zum Zwecke dieses Abschnitts zusammen als „Auftraggeber“ bezeichnet) am Datum der Zertifikatsausstellung entweder der Domain-Name-Registrant ist oder die Kontrolle über den FQDN besitzt.

Für die Prüfung der Domainkontrolle aller im Zertifikatsrequest enthaltenen Domain-Namen wird mindestens eine der folgenden Methoden eingesetzt:

3.2.2.4.1 Überprüfung, ob der Auftraggeber der Domain Kontakt ist

Nicht anwendbar.

3.2.2.4.2 Kontakt per E-Mail, Fax, SMS, oder Briefpost zum Domain Kontakt

Der Domain Kontakt wird per E-Mail, Fax, SMS oder Brief mit einem eindeutigen, einmaligen Zufallswert kontaktiert, der vom Domain Kontakt per E-Mail, Fax, SMS, oder Brief bestätigt werden muss. Die benötigten Kontaktdaten werden vom Domain-Name-Registrar abgefragt. (Verfahren nach Kapitel 3.2.2.4.2 der [CABF-BR]). Es gilt:

- Ein(e) E-Mail, Fax, SMS oder Postsendung kann die Berechtigung für mehrere Autorisierungs-Domain-Namen bestätigen.
- Die erstellte E-Mail, Fax, SMS oder Postsendung kann an mehrere Empfänger gesendet werden, vorausgesetzt, dass dieser Empfänger für den zu validierenden FQDN vom Registrar des Domain-Namens als Vertreter des Registranten des Domain-Namens aufgeführt wird.
- Der Zufallswert der per E-Mail, Fax, SMS oder Postsendung versendet wird ist einmalig.
- Ein(e) E-Mail, Fax, SMS oder Postsendung kann, einschließlich der Wiederverwendung des Zufallswertes, erneut versenden werden. Voraussetzung dafür ist, dass der gesamte Inhalt und die Empfänger unverändert bleiben.
- Der Zufallswert bleibt für die Verwendung in einer Bestätigungsantwort maximal 30 Tage nach seiner Erstellung gültig.

Sobald der FQDN mit dieser Methode validiert wurde, dürfen auch Zertifikate für andere FQDN ausgestellt werden, die mit allen Labels des validierten FQDN enden.

Diese Methode wird auch für die Validierung von Wildcard-Domain-Namen eingesetzt.

3.2.2.4.3 Telefonischer Kontakt zum Domain Kontakt

Nicht anwendbar.

3.2.2.4.4 Konstruierte E-Mail zum Domain Kontakt

Es wird bestätigt, dass der Auftraggeber die Kontrolle über die Domain hat, indem eine E-Mail an eine oder mehrere Adressen gesendet wird, die unter Verwendung von vorangestellten ‚admin', ‚administrator', ‚webmaster', ‚hostmaster' oder ‚postmaster', gefolgt von dem at-Zeichen („@"), gefolgt vom Domain-Namen des zu prüfenden FQDN. Die Antwort-E-Mail muss den Zufallswert enthalten. (Verfahren nach Kapitel 3.2.2.4.4 der [CABF-BR]). Es gilt:

- Jede E-Mail kann die Berechtigung für mehrere FQDN bestätigen, vorausgesetzt, dass der in der E-Mail verwendete Autorisierungs-Domain-Name ein Autorisierungs-Domain-Name für jeden FQDN ist, der bestätigt wird.
- Der Zufallswert ist in jeder E-Mail einmalig.
- Die E-Mail darf in ihrer Gesamtheit, einschließlich der Wiederverwendung des Zufallswertes, erneut versendet werden, vorausgesetzt, dass ihr gesamter Inhalt und Empfänger unverändert bleiben.
- Der Zufallswert bleibt für die Verwendung in einer Bestätigungsantwort maximal 30 Tage nach seiner Erstellung gültig.

Sobald der FQDN mit dieser Methode validiert wurde, dürfen auch Zertifikate für andere FQDNs ausgestellt werden, die mit allen Labels des validierten FQDN enden.

Diese Methode wird auch für die Validierung von Wildcard-Domain-Namen eingesetzt.

3.2.2.4.5 Domainvollmacht

Nicht anwendbar.

3.2.2.4.6 Vereinbarte Änderung auf der Webseite

Nicht anwendbar.

3.2.2.4.7 Änderung im DNS

Bei diesem Validierungsverfahren wird die Domainkontrolle durch das gezielte Einfügen von eindeutigen Informationen im DNS nachgewiesen:

- Es wird ein einmaliger, konstruierter Zufallswert verwendet.
- Der Zufallswert ist maximal 30 Tage nach seiner Erstellung gültig.
- Der Empfänger fügt den Zufallswert im DNS des zu prüfenden FQDN ein.

Sobald der FQDN mit dieser Methode validiert wurde, dürfen auch Zertifikate für andere FQDNs ausgestellt werden, die mit allen Labels des validierten FQDN enden.

Diese Methode wird auch für die Validierung von Wildcard-Domain-Namen eingesetzt. (Verfahren nach Kapitel 3.2.2.4.7 der [CABF-BR]).

3.2.2.4.8 IP-Adresse

Nicht anwendbar.

3.2.2.4.9 Testzertifikat

Nicht anwendbar.

3.2.2.4.10 TLS unter Verwendung einer Zufallszahl

Nicht anwendbar.

3.2.2.4.11 Jede andere Methode

Nicht anwendbar.

3.2.2.4.12 Validierung des Antragstellers als Domain-Kontakt

Durch Validierung des Antragstellers wird überprüft, ob der Antragsteller der Domain-Kontakt des beauftragten FQDN ist. Diese Methode kann nur verwendet werden, wenn die Zertifizierungsstelle auch der Domain Name Registrar oder ein verbundenes Unternehmen des Registrars des Haupt-Domain-Namens ist.

Hinweis: Sobald der vollqualifizierte Domänenname mit dieser Methode validiert wurde, kann die CA auch Zertifikate für andere vollqualifizierte Domänennamen ausstellen, die mit allen Bezeichnungen des validierten vollqualifizierten Domänennamens enden. Diese Methode eignet sich zur Validierung von Wildcard-Domainnamen.

Ein Vertrag mit dem Domain-Management der Deutschen Telekom AG (Registrar) enthält eine Liste mit festgelegten Domains, die im Besitz des Telekom Konzerns sind und von definierten Konzerneinheiten verwendet werden dürfen. Der beauftragte FQDN eines internen Auftraggebers wird gegen diese Liste geprüft.

Bei internen Aufträgen aus anderen Konzerneinheiten läßt sich der Registrierungsmitarbeiter den Auftraggeber als berechtigten Domain-Kontakt vom Domain-Management bestätigen.

3.2.2.4.13 E-Mail an DNS-CAA-Kontakt

Nicht anwendbar.

3.2.2.4.14 E-Mail an DNS-TXT-Kontakt

Nicht anwendbar.

3.2.2.4.15 Telefonkontakt mit Domänenkontakt

Nicht anwendbar.

3.2.2.4.16 Telefonkontakt mit DNS-TXT-Telefonkontakt

Nicht anwendbar.

3.2.2.4.17 Telefonkontakt mit DNS-CAA-Telefonkontakt

Nicht anwendbar.

3.2.2.4.18 Vereinbarte Änderung auf der Webseite - v2

Die Kontrolle über den FQDN wird nachgewiesen indem geprüft wird, ob der Auftraggeber einen Request Token im Inhalt einer Datei auf der Webseite abgelegt hat. Dies passiert Mittels einer HTTP-Anfrage. In dieser Anfrage erscheint der Request Token nicht.

Die Antwort wird akzeptiert, wenn die HTTP-Antwort den Statuscode 2xx enthält.

Die Datei, die den Request Token enthält

- wird über den Domänennamen, welche für die Autorisierung des FQDN benutzt wird, abgefragt, und
- wird aus dem Pfad "/.well-known/pki-validation/serverpassdv.txt" ausgelesen, und

- wird entweder über das "HTTPS"- oder "HTTP"-Schema und über den Port 443 oder 80 abgerufen.

Umleitungen werden verfolgt, wenn

- diese auf HTTP-Protokollebene initiiert werden, und
- die HTTP-Antwort den Statuscode 3xx enthält, und
- die Umleitungen zu Ressourcen-URLs, welche über das "HTTPS"- oder "HTTP"-Schema und über den Port 443 oder 80 abgerufen werden können, führen.

Der Request Token enthält einen Zeitstempel, einen eindeutigen Zufallswert und ggf. eine Referenznummer. Der Request Token ist maximal 30 Tage nach seiner Erstellung gültig.

Nachdem der FQDN mit dieser Methode validiert wurde, können Zertifikate auch für andere FQDNs, welche mit allen Labels des validierten FQDN enden, ausgestellt werden.

Diese Methode wird auch für die Validierung von Wildcard-Domain-Namen eingesetzt.

3.2.2.4.19 Vereinbarte Änderung auf der Webseite - ACME

Nicht anwendbar.

3.2.2.4.20 TLS Using ALPN (Application-Layer Protocol Negotiation)

Nicht anwendbar.

3.2.2.5 Überprüfung der Berechtigung oder der Kontrolle einer IP-Adresse

Dieses Kapitel beschreibt die erlaubten Prozesse und Verfahren um festzustellen, dass der Auftraggeber (oder die Muttergesellschaft, die Tochtergesellschaft oder das verbundene Unternehmen des Auftraggebers, zum Zwecke dieses Abschnitts zusammen als „Auftraggeber“ bezeichnet) im Besitz ist oder die Kontrolle einer im Zertifikat enthaltenen IP-Adresse ist. Vor der Zertifikatsausstellung wird bestätigt, dass jede enthaltene IP-Adresse mit mindesten einer der folgenden Verfahren geprüft wurde.

Es wird geprüft, dass der Auftraggeber für jede, in einem Zertifikat aufgelistete IP-Adresse, zum Zeitpunkt der Zertifikatsausstellung der Besitzer ist oder die Kontrolle hat.

3.2.2.5.1 Vereinbarte Änderung der Website

Es wird geprüft, ob der Auftraggeber für die beauftragte IP-Adresse die praktische Kontrolle nachzuweisen kann, indem er eine vereinbarte Änderung auf einer Webseite vornimmt. (Verfahren nach Kapitel 3.2.2.5.1 der [CABF-BR]).

Für den Nachweis ist eine bestimmte einmalige Textdatei unter einem vorgegebenen Pfad auf dem Server abzulegen (/.well-known/pki-validation/serverpassdv.txt).

- Die Zertifizierungsstelle muss per HTTP/HTTPS darauf zugreifen können.
- Es wird ein einmaliger, konstruierter Zufallswert verwendet
- Der Zufallswert ist maximal 30 Tage nach seiner Erstellung gültig.
- Der Empfänger fügt den Zufallswert an der definierten Stelle ein

3.2.2.5.2 E-Mail, Fax, SMS oder Brief an den IP-Adresskontakt

Der IP-Adresskontakt wird per E-Mail, Fax, SMS oder Brief mit einem eindeutigen, einmaligen Zufallswert kontaktiert, der vom IP-Adresskontakt per E-Mail, Fax, SMS, oder Brief bestätigt werden muss. Die benötigten Kontaktdaten werden vom Domain-Name-Registrar abgefragt. (Verfahren nach Kapitel 3.2.2.5.2 der [CABF-BR]).

Es gilt:

- Ein(e) E-Mail, Fax, SMS oder Postsendung kann die Berechtigung für mehrere IP-Adressen bestätigen.
- Die erstellte E-Mail, Fax, SMS oder Postsendung kann an mehrere Empfänger gesendet werden, vorausgesetzt, dass dieser Empfänger für die zu validierende IP-Adresse bei der Registrierungsstelle aufgeführt ist.
- Der Zufallswert der per E-Mail, Fax, SMS oder Postsendung versendet wird ist einmalig.
- Ein(e) E-Mail, Fax, SMS oder Postsendung kann, einschließlich der Wiederverwendung des Zufallswertes, erneut versenden werden. Voraussetzung dafür ist, dass der gesamte Inhalt und die Empfänger unverändert bleiben.
- Der Zufallswert bleibt für die Verwendung in einer Bestätigungsantwort maximal 30 Tage nach seiner Erstellung gültig.

3.2.2.5.3 Rückwärtssuche der IP-Adresse

Die Kontrolle über die IP-Adresse wird bestätigt, indem zunächst durch die Rückwärtssuche ein zugeordneter Domainname gefunden wird und anschließend die Überprüfung mittels der zulässigen Verfahren aus Kapitel 3.2.2.4 durchgeführt wird. (Verfahren nach Kapitel 3.2.2.5.3 der [CABF-BR]).

3.2.2.5.4 Andere Methoden

Nicht anwendbar.

3.2.2.5.5 Telefonischer Kontakt zum IP-Adresskontakt

In dem Telefonat lässt sich die CA vom IP-Adresskontakt den Zertifikatsantrag für jede IP-Adresse bestätigen. (Verfahren nach Kapitel 3.2.2.5.5 der [CABF-BR]).

3.2.2.5.6 ACME “http-01” Method für IP-Adressen

Nicht anwendbar.

3.2.2.5.7 ACME “tls-alpn-01” Methode für IP-Adressen

Nicht anwendbar.

3.2.2.6 Überprüfen einer Wildcard Domain

Das Wildcard-Zeichen (*, Sternchen, Asterisk) wird nur ganz links im FQDN akzeptiert. Wildcard-Zeichen in Verbindung mit Zeichen und/oder Buchstaben (z.B. h*l.example.com) sowie mehr als ein Wildcard-Zeichen (z.B. *.*.example.com) pro FQDN werden nicht akzeptiert.

Wenn ein Wildcard-Zeichen in einem Label unmittelbar links von einem „registry-controlled“ oder „public suffix“ erscheint, wird die Ausstellung abgelehnt (z.B. „*.co.uk“ oder „*.de“), es sei denn, der Auftraggeber weist seine rechtmäßige Kontrolle über den gesamten Domain-Namensraum nach.

3.2.2.7 Zuverlässigkeit der Datenquelle

Es werden ausschließlich Datenquellen und Datenbanken Dritter berücksichtigt, die als hinreichend zuverlässig eingestuft wurden. Es werden keine ausschließlich selbstgepflegten oder von verbundenen Unternehmen geführten Datenquellen verwendet.

3.2.2.8 CAA Records

Siehe Kapitel 3.2.5.2 und 4.2.2.

3.2.3 Authentifizierung der Identität von Endteilnehmern

3.2.3.1 Organisationprüfung

3.2.3.1.1 TeleSec ServerPass Standard und SAN/UCC:

Um die Juristische Person, die im Subject Distinguished Name (subjectDN) des Zertifikats unter Organization (O) genannt wird, zu bestätigen, wird entsprechend der Art der juristischen Person bei der Erstbeauftragung folgendes Dokument benötigt:

Juristische Person:

Das von einem Unterschrifts- oder durch Vollmachtberechtigten der Organisation unterschriebene Auftragsformular.

Behörde:

Das von einem Bevollmächtigten der Behörde unterschriebene und mit dem Dienstsiegel versehene Auftragsformular.

Verein:

Die beglaubigte Kopie (nicht älter als 30 Tage) des Vereinsregisterauszuges ist zusammen mit dem unterzeichneten Auftragsformular einzureichen.

Gewerbetreibende(r):

Die beglaubigte Kopie (nicht älter als 30 Tage) eines aktuellen Gewerbescheins und des Personalausweises des Gewerbetreibenden ist zusammen mit dem unterschriebenen Auftragsformular einzureichen.

Für alle Gesellschaftsformen wird Folgendes geprüft:

- die Angaben des Auftragsformulars sind identisch mit den Angaben im Certificate Signing Request (CSR) des Online-Auftrags,
- der Firmenname der Organisation / des Unternehmens im Feld O = OrganizationName stimmt mit den Daten zur Organisation und der Eintragung im elektronischen Handelsregister (bei deutschen Organisationen) oder vergleichbarer Verzeichnisse (z.B. entsprechend der ausländischen Jurisdiktion, Vereinsregister) überein. Eventuell werden zusätzliche, aktuelle Organisationsdokumente (nicht älter als 30 Tage), die von einer zuständigen Stelle oder Behörde ausgestellt wurden und die Existenz der Organisation (z.B. Vereinsregister oder vergleichbares Dokument, Dienstsiegel) bestätigen, benötigt.
- die im Zertifikatsauftrag angegebene Adresse der Organisation wird anhand des elektronischen Handelsregisters oder vergleichbarer Verzeichnisse überprüft. Der Auftraggeber muss an dem angegebenen Standort eine Filiale, Geschäftsstelle oder ähnliches betreiben.
- Die Autorisierung des verantwortlichen Ansprechpartners der im Auftrag aufgeführten Organisation (juristische Person),
- Im Falle, dass ein Dritter im Namen der Organisation die Zertifikatsbeauftragung/ -verwaltung für diese durchführt, bedarf es einer entsprechenden, schriftlichen Vollmacht über die Übertragung der Rechte,

Für die Überprüfung der Existenz oder der Adresse der Organisation können alternativ oder zusätzlich zum Handelsregister bzw. der vergleichbaren Verzeichnisse weitere Methoden herangezogen werden. Bei Bedarf kann ein Dun & Bradstreet-Report als vertrauenswürdige, verlässliche und unabhängige Datenquelle verwendet werden.

Als weitere Methode zur Überprüfung ist die Vorlage einer von einer entsprechend qualifizierten Person ausgestellten anwaltlichen Stellungnahme zulässig. Ebenso kann ein Mitarbeiter der Zertifizierungsstelle oder ein von ihr beauftragter Dritter den angegebenen Standort persönlich aufsuchen und bestätigen.

Zusätzliche Prüfungen werden nach Bedarf durchgeführt.

3.2.3.1.2 TeleSec ServerPass EV/EV SAN:

Die erforderlichen Prüfungen werden gemäß [CABF-BREV] durchgeführt.

3.2.3.2 Identitätsprüfung einer natürlichen Person

Der Auftraggeber für TeleSec ServerPass muss eine juristische Person sein, d.h. es wird kein Zertifikat für eine natürliche Person ausgestellt.

3.2.4 Nicht überprüfte Teilnehmerangaben

Das TeleSec ServerPass-Zertifikat beinhaltet keine ungeprüften Angaben.

3.2.5 Überprüfung der Berechtigung

Falls der Antragsteller nicht der Zertifikatsinhaber ist, wird der vollständige Name und die Berechtigung des Antragstellers, im Namen des Zertifikatsinhabers zu agieren, überprüft.

Zur Vermeidung von Interessenskonflikten müssen der TSP und der Antragsteller unterschiedliche Entitäten sein. Als einzige Ausnahme gilt der TSP selbst, wenn dieser TLS-Zertifikate für eigene Server beauftragt.

3.2.5.1 Sicherstellung der Authentizität des Zertifikatauftrages

3.2.5.1.1 TeleSec ServerPass Standard und SAN/UCC:

Jeder ServerPass Kunde schließt mit der Deutschen Telekom Security GmbH einen Vertrag über die entsprechende Dienstleistung ab. Der Vertreter des Kunden, welcher den Vertrag unterzeichnet, ist dem Trust Center namentlich bekannt.

Zur Feststellung der Authentizität der Zertifikaterstbeauftragung erfolgt ein Anruf bei der zentralen Telefonnummer des Kunden, welche im Handelsregister oder einem vergleichbaren Verzeichnis hinterlegt ist. Der durchführende RA-Mitarbeiter lässt sich von der Zentrale mit dem oben genannten Vertreter des Kunden verbinden. Dieser bestätigt die Authentizität des Zertifikatauftrages, d.h. er bestätigt, dass die beauftragende Person ein autorisierter Vertreter des Antragstellers ist.

3.2.5.1.2 TeleSec ServerPass EV/EV SAN:

Die Überprüfung der Berechtigung erfolgt gemäß den EV-Guidelines [ETSI EV].

3.2.5.1.3 TeleSec ServerPass EV/EV SAN mit Q-Vermerk (QWAC, QCP-w)

Zusätzlich zu den oben beschriebenen Prüfungen ist für die Ausstellung eines qualifizierten Website-Zertifikats (QWAC, QCP-w) die persönliche Identifizierung per POSTIDENT eines Vertreters der juristischen Person verpflichtend.

3.2.5.2 Prüfung von CAA Einträgen im DNS

Im Rahmen der Berechtigungsprüfung werden alle FQDN-Einträge unmittelbar vor der Zertifikatsausstellung gegen CAA Einträge im DNS geprüft (Certification Authority Authorization; CAA Records for Fully Qualified Domain Names).

Wenn ein oder mehrere CAA Resource Records gefunden werden, von denen kein issue- bzw. issuewild-Property „telesec.de“ enthält, dann wird der Zertifikatsauftrag abgelehnt. Enthält das issuewild-Property ein Semikolon „;“, dann wird ein Wildcard-Zertifikatsauftrag immer abgelehnt.

Wenn kein CAA Resource Record hinterlegt wurde oder dessen issue- bzw. issuewild-Property „telesec.de“ enthält, dann wird der Prüfprozess fortgesetzt.

Es werden 8 CNAME-Ketten-Einträge verarbeitet und die Länge der Kette wie empfohlen auf maximal 10 begrenzt.

3.2.6 Kriterien für Interoperabilität

Nicht anwendbar.

3.3 Identitätsprüfung und Authentifizierung bei einer Zertifikatserneuerung

3.3.1 TeleSec ServerPass Standard und SAN/UCC:

Die Zertifikatserneuerung erfolgt ausschließlich im Serviceportal und kann nur vom autorisierten Kunden beauftragt werden. Der Nachweis der Identität und Authentizität erfolgt anhand der korrekten Zugangsdaten sowie des für die Erneuerung erforderlichen Service-Passwortes.

Die durchzuführenden Überprüfungen (Identität, Adresse, Berechtigungen) entsprechen prinzipiell den Verfahren bei der Erstbeauftragung (siehe Kapitel 3.2.2). Dabei kann auf bereits vorliegende Dokumente und Informationen zurückgegriffen werden. Für eine Zertifikatserneuerung ist es weder erforderlich den Erneuerungs-Auftrag zu unterschreiben noch den Auftrag an das Trust Center zu senden. Der Ausdruck des Auftrags dient lediglich zur Vervollständigung der Unterlagen des Auftraggebers.

3.3.2 TeleSec ServerPass EV/EV SAN:

Eine Zertifikatserneuerung findet bei ServerPass EV/EV SAN nicht statt. Stattdessen erfolgt eine Neubeauftragung nach Kapitel 3.2.2.

Die Zertifizierungsstelle verwendet für die Validierung eines Erneuerungsauftrags ausschließlich Dokumente, Unterlagen oder sonstige Informationen, die bei der Ausstellung des Zertifikats nicht älter als 13 Monate sind.

3.3.3 Identifizierung und Authentifizierung für routinemäßige Schlüsselerneuerung

3.3.3.1 TeleSec ServerPass Standard und SAN/UCC:

Die routinemäßige Schlüsselerzeugung obliegt der Verantwortung des Kunden. Die Schlüsselerneuerung kann im Rahmen der Zertifikatserneuerung im Serviceportal durchgeführt und nur vom autorisierten Kunden beauftragt werden. Die Prüfung der Identität und Authentizität erfolgt anhand der korrekten Zugangsdaten sowie des, für die Erneuerung erforderlichen Service-Passwortes.

3.3.3.2 TeleSec ServerPass EV/EV SAN:

Eine routinemäßige Schlüsselerneuerung findet nicht statt.

3.3.4 Identitätsprüfung bei Schlüsselerneuerung nach Zertifikatssperrung

Die Schlüsselerneuerung eines gesperrten Zertifikats ist nicht möglich.

3.4 Identifizierung und Authentifizierung bei Sperraufträgen

Über das Serviceportal <myServerPass> können autorisierte Endteilnehmer ihre Zertifikate selbst sperren.

Nachdem das zu sperrende Zertifikat selektiert wurde, muss der Sperrwunsch durch die Angabe des Zertifikat-Service-Passwortes bestätigt und die Sperrung durchgeführt werden.

Neben der Generierung eines Sperrauftrags durch den Endteilnehmer behält sich die Zertifizierungsstelle das Recht vor, bei Missbrauch oder Missbrauchsverdacht Zertifikatssperrungen durchzuführen, (siehe auch Kapitel 4.9.1.1, 4.9.2, und 4.9.3 ff).

Die begründete und gewollte Sperrung eines Zertifikats ist endgültig.

3.4.1 Sperrwunsch bei Erkennen von missbräuchlichem Einsatz

Falls der Verdacht auf missbräuchlichen Einsatz eines Trust Center Zertifikats besteht, kann dies unter Angabe der Aussteller-CA und der Seriennummer des Zertifikats sowie der Beschreibung des Missbrauchs dem Servicedesk mitgeteilt werden. Diese Fälle werden an das Trust Center weitergeleitet. Es werden geeignete Prüfmaßnahmen eingeleitet. Bestätigt sich ein begründeter missbräuchlicher Zertifikatseinsatz, dann kann die Zertifizierungsstelle dieses Zertifikat sperren.

Für die Kontaktaufnahme für die Meldung eines Zertifikatsmissbrauchs sind die folgenden Eingangskanäle zu verwenden:

Internet: https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden/

E-Mail: telesec_support@t-systems.com

4 BETRIEBLICHE ANFORDERUNGEN IM LEBENSZYKLUS VON ZERTIFIKATEN

4.1 Zertifikatsauftrag

4.1.1 Berechtigte Auftraggeber

TeleSec ServerPass stellt Zertifikate nur für juristische Personen (Auftraggeber) aus:

- Unternehmen,
- Behörden,
- private Organisationen oder
- nichtkommerzielle Unternehmen.

Dies sind z.B. Stiftungen bürgerlichen Rechts, Körperschaften des Privatrechts wie Aktien Gesellschaften, eingetragene Vereine, Gesellschaften mit beschränkter Haftung, eingetragene Genossenschaften.

Der Auftraggeber muss folgende Rollen benennen:

- verantwortlicher Ansprechpartner
  Der verantwortliche Ansprechpartner ist berechtigt, im Namen des Auftragsgebers zu handeln. Telekom Security ist verpflichtet den verantwortlichen Ansprechpartner anhand des Handelsregisterauszuges (HRA), oder vergleichbaren Verzeichnissen, zu verifizieren. Sollte der verantwortlicher Ansprechpartner nicht im HRA aufgeführt sein, wird eine entsprechende Vollmacht benötigt, die wiederum von einer im HRA gelisteten Person unterzeichnet sein muss.

- technischer Ansprechpartner
  Diese Person ist die Kontaktperson für Telekom Security. Sie ist berechtigt, die Beauftragung des Zertifikates vorzunehmen, das ausgestellte Zertifikat herunter zu laden, das Zertifikat und die Kundendaten zu verwalten. Der techn. Ansprechpartner kann auch bei einem ISP oder einem Hosting-Unternehmen beschäftigt sein. Die Vertretungsberechtigung muss dann in Form einer Handlungsvollmacht vorliegen.

- kaufmännischer Ansprechpartner
  Diese Person ist der Adressat bei der Rechnungslegung und wird kontaktiert, wenn es Probleme bzgl. der Abrechnung gibt.

- Bearbeiter (Stellvertreter des technischen Ansprechpartners):
  Bearbeiter können vom technischen Ansprechpartner zu dessen Unterstützung angelegt werden. Bearbeiter haben die gleichen Berechtigungen wie der technische Ansprechpartner, außer der Verwaltung von Bearbeitern.

- administrativer Ansprechpartner (nur bei EV-Zertifikaten)
  Diese Person ist vertretungsberechtigt, als Zertifikatsgenehmiger zu handeln. Der Zertifikatsgenehmiger genehmigt Zertifikatsaufträge die durch den technischen Ansprechpartner erstellt wurden. Der Zertifikatsgenehmiger kann auch die Rolle des technischen Ansprechpartners einnehmen, oder andere damit beauftragen, die Rolle des technischen Ansprechpartners zu übernehmen. Im Rahmen des Authentifizierungs-Prozesses wird sich Telekom Security mit dem Zertifikatsgenehmiger in Verbindung setzen, um die Angaben des Zertifikatsauftrages und die Vertretungsberechtigung zu

verifizieren. Die Vertretungsberechtigung muss in Form einer Handlungsvollmacht vorliegen.

- zeichnungsberechtigter Ansprechpartner (nur bei EV-Zertifikaten)
  Der zeichnungsberechtigte Ansprechpartner entspricht dem verantwortlichen Ansprechpartner bei EV-Zertifikaten.

Der Auftraggeber darf eine Person mit mehreren der aufgeführten Rollen betrauen.

4.1.2 Auftragsprozess und Verantwortlichkeiten

4.1.2.1 Endteilnehmer

Der Endteilnehmer (Auftraggeber) muss vor dem Absenden des Auftrags die Datenschutzhinweise, die Allgemeinen Geschäftsbedingungen TeleSec-ServerPass [AGB], die ServerPass Leistungen und Nutzungsbedingungen, das TeleSec ServerPass CPS sowie die Leistungsbeschreibung und Preise akzeptieren.

Ferner sichert der Endteilnehmer zu:

- dass die im Zertifikatsauftrag gemachten Angaben wahr und korrekt sind,
- ein Schlüsselpaar zu generieren oder die Generierung zu beauftragen,
- seinen öffentlichen Schlüssel mit seinen Zertifikatsdaten an die Zertifizierungsstelle im PKCS#10-Format zur Zertifikatserzeugung zu übermitteln.

Durch diese Zertifikatsbeauftragung schließt der ServerPass Kunde (Auftraggeber) einen Vertrag mit der Deutschen Telekom Security GmbH über ein Endteilnehmer-Zertifikat ab. Die Vereinbarungen des Vertrags bzw. die Zustimmung zu den Nutzungsbedingungen werden für jede erneute Beauftragung, Erneuerung oder Re-Issue wiederholt.

4.2 Bearbeitung der Zertifikatsaufträge

Die folgende Prozessbeschreibung gilt auch für den TSP selbst, wenn dieser TLS-Zertifikate für eigene Server beauftragt.

4.2.1 Initiale und einmalige Vorarbeiten

Initial schließt jeder ServerPass Kunde mit der Deutschen Telekom Security GmbH einen Vertrag über die entsprechende Dienstleistung ab.

4.2.1.1 Bedingungen

Falls der Zertifikatsnehmer und die ausstellende CA einer gemeinsamen juristischen Person angehören (affiliate), muss der Repräsentant des Antragstellers vor der Ausstellung eines Zertifikates die Nutzungsbedingung akzeptieren. Ist der Zertifikatsnehmer kein Konzernunternehmen (beauftragte Drittpartei oder non affiliate), muss der Antragsteller die Allgemeinen Geschäftsbedingungen TeleSec-ServerPass [AGB] und die Nutzungsbedingungen für ServerPass in einer rechtlich durchsetzbaren Form vereinbaren.

Sowohl die Nutzungsbedingung als auch die Allgemeinen Geschäftsbedingungen TeleSec-ServerPass [AGB] werden über ein entsprechendes elektronisches Formular im ServerPass Serviceportal ausgeführt.

Die Vereinbarung des Bezugsvertrages bzw. die Zustimmung zu den Nutzungsbedingungen wird für jede erneute Beauftragung, Renewal oder Re-Issue wiederholt.

4.2.1.2 Durchführung der Identifikation und Authentifizierung

Die Zertifizierungsstelle verwendet für die Validierung eines Auftrags ausschließlich Dokumente, Unterlagen oder sonstige Informationen, die bei der Ausstellung eines Zertifikats nicht älter als 13 Monate sind.

Denied List (Schwarze Liste)

Das Trust Center unterhält eine interne Datenbasis, in die gesperrte Zertifikate eingehen, die in Zusammenhang mit Phishing-, Missbrauchs- oder Betrugsversuchen stehen. Diese Informationen werden verwendet, um zukünftige verdächtige Zertifikatsaufträge identifizieren zu können.

High Risk List

Im Trust Center werden sowohl Organisationen, als auch Domainnamen bzw. IP-Adressen in einer Datenbank gepflegt, die möglicherweise aufgrund ihrer Attraktivität Ziel von Phishing-, Missbrauchs- oder Betrugsattacken sein könnten. Diese Zertifikatsaufträge werden automatisch kenntlich gemacht, um die Registrierungsmitarbeiter auf die besondere Sorgfaltspflicht hinzuweisen. Dadurch soll zusätzliche Wachsamkeit und Aufmerksamkeit bei der Überprüfung der Auftragsdaten erzeugt werden. Die Prüfung kann im Einzelfall dazu führen, dass ein beauftragtes Zertifikat nicht ausgestellt wird.

4.2.1.2.1 TeleSec ServerPass Standard und SAN/UCC:

Die Identifizierung und Authentifizierung der erforderlichen Endteilnehmer-Informationen wird von der Zertifizierungsstelle gemäß Kapitel 3.2 durchgeführt.

4.2.1.2.2 TeleSec ServerPass EV/EV SAN:

Die Identifizierung und Authentifizierung der erforderlichen Endteilnehmer-Informationen wird von der Zertifizierungsstelle durchgeführt.

4.2.2 Genehmigung oder Ablehnung von Zertifikatsaufträgen

Werden alle erforderlichen Prüfungen aus Kapitel 3 erfolgreich durchlaufen, wird der Zertifikatsauftrag genehmigt und das Zertifikat ausgestellt.

Alle FQDN-Einträge werden unmittelbar vor der Ausstellung eines Zertifikats gegen CAA-Einträge im DNS geprüft. Sollte kein CAA Ressource Record hinterlegt sein oder dessen issue- bzw. issuewild-Property „telesec.de“ enthalten, wird die Ausstellung des Zertifikats fortgeführt. „iodef“-Einträge werden ausgewertet, jedoch nicht weiter verfolgt. Weitere Einträge des CAA-Records werden nicht unterstützt.

Durch die Vergabe einer Referenznummer bei der Zertifikatsbeauftragung wird die eindeutige Zuordnung von einem ausgestellten Zertifikat zu den entsprechenden Auftragsunterlagen und Zusatzdokumenten (z.B. Vollmachten) hergestellt.

Ein Zertifikatsauftrag muss abgelehnt werden, wenn:

- Der Auftrag nicht mindestens einen voll qualifizierten Domain-Namen oder eine IP-Adresse enthält, welche in die SAN-Erweiterung übernommen wird.
- Der Auftrag eine IP-Adresse/eine Top-Level-Domain aus einem reservierten Adressraum oder einen internen Server-/Hostnamen enthält.
- Der öffentliche Schlüssel die RSA-Mindestschlüssellänge von 2048 Bit unterschreitet.
- Die Untersuchung auf Debian-Schwäche positiv ausfällt.

- Für einen Neuauftrag ein öffentlicher Schlüssel verwendet werden soll, der bereits für ein anderes ServerPass-Zertifikat benutzt wird.
- Ein CAA Resource Record gefunden wird, dessen issue- bzw. issuewild-Property nicht „telesec.de“ beinhaltet.
- Nicht alle erforderlichen Prüfungen erfolgreich durchlaufen werden.

Das Trust Center überprüft regelmäßig (maximal alle 30 Tage) auf der ICANN-Website (https://newgtlds.icann.org), ob neue gTLD freigegeben oder gekündigt wurden. Im Falle von Änderungen erfolgt eine Überprüfung, ob Zertifikate für diese gTLD ausgestellt wurden und stellt eine weitere Zertifikatsausstellung ein, bis die Kontrolle über den Domainnamen oder das ausschließliche Recht des Auftraggebers zur Verwendung des Domain-Namens nachgewiesen wurde.

Wird ein Nachweis nicht erbracht oder die gTLD gekündigt, werden alle ausgestellten Zertifikate mit dieser TLD im Domainnamen innerhalb von 120 Tagen gesperrt (siehe Kap. 4.9.1.1).

Im Falle einer Zurückstellung oder Ablehnung des Auftrags wird der Beauftragte (Techn. Ansprechpartner) des Zertifikatsnehmers unter Angabe von Gründen per E-Mail benachrichtigt.

4.2.3 Bearbeitungsdauer von Zertifikatsaufträgen

Die Bearbeitung des Zertifikatauftrags erfolgt innerhalb eines angemessenen Zeitraums nach Erhalt der Beauftragung.

4.3 Ausstellung von Zertifikaten

4.3.1 Aktivitäten der CA während der Ausstellung von Zertifikaten

Der TSP stellt sicher, dass bei der Ausstellung der Zertifikate die Integrität und Authentizität gewährleistet wird. Technische, organisatorische und personelle Maßnahmen sorgen für den Schutz der Daten vor Fälschung bis zur Ausstellung der Zertifikate.

Durch die Vergabe einer Referenznummer bei der Zertifikatsbeauftragung wird die eindeutige Zuordnung von einem ausgestellten Zertifikat zu den entsprechenden Auftragsunterlagen und Zusatzdokumenten (z.B. Vollmachten) hergestellt.

Durch die Überprüfung der Signatur eines Schlüssels der mittels signiertem PKCS#10-Request übergeben wurde, stellt der TSP sicher, dass der Auftraggeber im Besitz der Schlüssel ist oder die Kontrolle darüber hat.

TeleSec ServerPass verwendet bei allen ausgestellten Zertifikaten Certificate Transparency.

Dies dient der Sicherheit und der Transparenz der Zertifikatsausstellung. Einzelheiten finden Sie unter https://www.certificate-transparency.org.

4.3.2 Benachrichtigung des Endteilnehmers über die Ausstellung eines Zertifikats

Der technische Ansprechpartner wird über die Ausstellung des Zertifikats per E-Mail informiert. Das ausgestellte Zertifikat wird im Serviceportal <myServerPass> unter ‚Meine Zertifikate’ gelistet und zum Herunterladen angeboten.

4.4 Zertifikatsannahme

4.4.1 Akzeptanz durch den Zertifikatsinhabers

Nach erfolgreicher Prüfung der Auftragsdaten wird das Zertifikat generiert. Gleichzeitig erfolgt die Versendung der Auftragsbestätigung, mit der der Vertrag zustande kommt.

Der Endteilnehmer muss vor der Nutzung des Zertifikats die darin angegebenen Informationen auf Richtigkeit überprüfen.

4.4.2 Veröffentlichung des Zertifikats durch die CA

Der Auftraggeber kann während der Zertifikatsbeauftragung entscheiden, ob sein Zertifikat in mehreren öffentlichen Certificate Transparency (CT) Logservern veröffentlicht wird.

Wichtiger Hinweis: Die Nichtveröffentlichung zieht eine Einschränkung des Leistungsumfangs nach sich und kann dazu führen, dass eine Applikation das Zertifikat nicht akzeptiert oder ablehnt.

4.4.3 Benachrichtigung anderer Stellen über die Zertifikatsausstellung durch die CA

Die Benachrichtigung weiterer Stellen ist nicht vorgesehen.

4.4.4 Certificate Transparency

TeleSec ServerPass unterstützt Certificate Transparency.

Alle ausgestellten Zertifikate enthalten per default die Erweiterung Certificate Transparency. Dies dient der Sicherheit und der Transparenz der Zertifikatsausstellung. Die CT-Erweiterung kann auf Kundenwunsch abgewählt werden. Einzelheiten finden Sie unter https://www.certificate-transparency.org.

4.5 Schlüssel- und Zertifikatsnutzung

4.5.1 Nutzung des Schlüsselpaars und des Zertifikats durch den Endteilnehmer

Das Zertifikat und der zugehörige private Schlüssel dürfen nur entsprechend den Allgemeinen Geschäftsbedingungen TeleSec-ServerPass [AGB], den Leistungen und Nutzungsbedingungen und den Anforderungen des vorliegenden CPS verwendet werden.

Endteilnehmer müssen ihren privaten Schlüssel vor unbefugtem Gebrauch schützen und dürfen den privaten Schlüssel nach dem Ablauf des Gültigkeitszeitraums oder der Sperrung des Zertifikats nicht mehr benutzen. Das Zertifikat darf ausschließlich für autorisierte und legale Zwecke in Übereinstimmung mit dem vorliegenden Dokument eingesetzt werden.

4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Vertrauende Dritte (Relying Parties)

Jeder Vertrauende Dritte, der ein Zertifikat nutzt, das von einer TeleSec ServerPass Sub-CA ausgestellt wurde, sollte

- vor der Nutzung des Zertifikats dessen Gültigkeit überprüfen, in dem er unter anderem die gesamte Zertifikatskette bis zum Wurzelzertifikat validiert (Zertifizierungshierarchie), den Gültigkeitszeitraum und die Sperrinformationen (CRL, OCSP) des Zertifikats überprüft,

- den technischen Verwendungszweck prüfen, der durch das im Zertifikat angezeigte Attribut „Schlüsselverwendung“ und „erweiterte Schlüsselverwendung“ festgelegt ist.

Vertrauende Dritte müssen geeignete Software (z.B. aktuellen Browser) zur Überprüfung von Zertifikaten (Validierung) und den damit verbundenen kryptografischen Verfahren verwenden.

4.6 Zertifikatserneuerung (Re-Zertifizierung)

4.6.1 TeleSec ServerPass Standard und SAN/UCC:

Um durchgehend authentische und sichere elektronische Kommunikation zu gewährleisten, muss die Erneuerung eines Zertifikats vor Ablauf der Gültigkeit erfolgen, das bedeutet, dass nur gültige Zertifikate erneuert werden können. Die Zertifikatserneuerung basiert auf den bestehenden Zertifikatsdaten, eine erneute Registrierung ist nicht vorgesehen. Bei einer Zertifikatserneuerung wird auf Basis des gleichen Subject-DN (Kapitel 3.1.1.1) ein neues Zertifikat generiert, das einen neuen Gültigkeitszeitraum und eine neue Seriennummer besitzt. Der Auftraggeber kann selbst entscheiden, ob für die Zertifikatserneuerung ein neuer öffentlicher Schlüssel eines neu generierten Schlüsselpaares oder der alte Schlüssel weiter verwendet werden soll.

Bei der weiteren Verwendung des alten Schlüsselpaares wird vorausgesetzt, dass die eindeutige Zuordnung von Zertifikatsnehmer und Schlüssel gewährleistet ist, keine Kompromittierung des Schlüssels vorliegt und die kryptografischen Parameter (z.B. Schlüssellänge) für die Gültigkeitsdauer des neuen Zertifikats noch ausreichend sind.

4.6.2 Umstände für eine Zertifikatserneuerung

4.6.2.1 TeleSec ServerPass Standard und SAN/UCC:

Eine Zertifikatserneuerung ist jederzeit während der Laufzeit des aktuellen Zertifikats möglich. Abgelaufene Zertifikate sind nicht erneuerbar. Das nicht mehr benötigte Zertifikat ist umgehend zu sperren.

4.6.2.2 TeleSec ServerPass EV/EV SAN:

Eine Zertifikatserneuerung wird derzeit nicht angeboten. Im Serviceportal <myServerPass> kann stattdessen eine Neubeauftragung mit ähnlichem Komfort wie eine Zertifikatserneuerung initiiert werden.

4.6.3 Antragsberechtigte für eine Zertifikatserneuerung

Siehe Kap. 4.1.1

4.6.4 Bearbeitung von Anträgen auf Zertifikatserneuerung

Die Beauftragung für eine Zertifikatserneuerung wird automatisiert geprüft und nach erfolgreicher Prüfung aller relevanten Daten automatisch freigegeben. Zugrundeliegende Dokumente und Daten dürfen hierbei nicht älter 13 Monate sein. Im Zuge dieser Beauftragung muss der Auftraggeber den aktuell gültigen Vertragsbedingungen (z.B. AGB, Leistungsbeschreibung, Nutzungsbedingungen, etc.) zustimmen.

Bei nicht erfolgreicher automatisierter Prüfung erfolgt keine automatisierte Freigabe und es wird eine manuelle Bearbeitung durch den TSP durchgeführt.

4.6.5 Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines neuen Zertifikats

Siehe Kap. 4.3.2.

4.6.6 Annahme einer Zertifikatserneuerung

Siehe Kap. 4.4.1.

4.6.7 Veröffentlichung einer Zertifikatserneuerung durch die CA

Siehe Kap. 4.4.2.

4.6.8 Benachrichtigung weiterer Stellen über eine Zertifikatserneuerung durch die CA

Siehe Kap. 4.4.3.

4.7 Zertifikatserneuerung mit neuem Schlüssel (Re-Keying)

TeleSec ServerPass Standard und SAN/UCC:

Beim Re-Key Prozess wird mit dem Zertifikatsrequest ein neuer öffentlicher Schlüssel verwendet. Grundvoraussetzung dafür ist die Erzeugung eines neuen Schlüsselpaars. Zertifikatsinhalt und Identifikationsdaten bleiben unverändert.

Ob Re-Key für die verwendete Anwendung möglich ist, oder ob das „alte“ Schlüsselpaar und damit der „alte“ öffentliche Schlüssel wiederverwendet werden muss, hängt von den technischen Vorgaben der Anwendung (z.B. Webserver) ab und obliegt der Verantwortung des Kunden.

Bei der Zertifikatserneuerung (Kapitel 4.6) und bei Re-Issue (Kapitel 4.7.8) kann eine Schlüsselerneuerung beauftragt werden.

4.7.1 Bedingungen für eine Schlüsselerneuerung

4.7.1.1 TeleSec ServerPass Standard und SAN/UCC:

Die Zertifikatserneuerung mit Schlüsselerneuerung kann jederzeit während der Laufzeit des aktuellen Zertifikats und ausschließlich vom autorisierten Kunden durchgeführt werden. Das aktuelle Zertifikat darf nicht gesperrt und nicht ungültig/abgelaufen sein.

4.7.1.2 TeleSec ServerPass EV/EV SAN:

Eine Schlüsselerneuerung (Re-Key) wird derzeit nicht angeboten.

4.7.2 Antragsberechtigte für ein Re-Issue

Siehe Kap. 4.1.1.

4.7.3 Verarbeitung von Schlüsselerneuerungsaufträgen

4.7.3.1 TeleSec ServerPass Standard und SAN/UCC:

Wenn der autorisierte Endkunde die Schlüsselerneuerung im Rahmen der Zertifikatserneuerung oder dem Zertifikat-Re-Issue nach Eingabe des Service-Passwortes

abgesendet hat, wird das Zertifikat nach erfolgreicher Prüfung aller relevanten Daten ausgestellt. Im Zuge dieser Beauftragung muss der Auftraggeber den aktuell gültigen Vertragsbedingungen (z.B. AGB, Leistungsbeschreibung, Nutzungsbedingungen, etc.) zustimmen.

Bei nicht erfolgreicher automatisierter Prüfung erfolgt keine automatisierte Freigabe und es wird eine manuelle Bearbeitung durch den TSP durchgeführt.

4.7.4 Benachrichtigung des Endteilnehmers über die Ausstellung eines erneuerten Zertifikats

Es gelten die Regelungen gemäß Kap. 4.3.2.

4.7.5 Annahme einer Zertifikatserneuerung mit neuem Schlüsselmaterial

Siehe Kap. 4.4.1

4.7.6 Veröffentlichung erneuerter Zertifikate durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kap. 4.4.2.

4.7.7 Information Dritter über die Ausstellung neuer Zertifikate durch die Zertifizierungsstelle

Es gelten die Regelungen gemäß Kap. 4.4.3.

4.7.8 Zertifikat erneut ausstellen (Re-Issue)

4.7.8.1 TeleSec ServerPass Standard und SAN/UCC:

Um durchgehend authentische und sichere elektronische Kommunikation zu unterstützen, wird unter bestimmten Umständen die Möglichkeit angeboten, für die Restlaufzeit des bestehenden Zertifikats eine erneute Zertifikatsausstellung (Re-Issue) durchzuführen.

Dieser Fall liegt dann vor, wenn beispielsweise durch einen Defekt des Webservers oder einen Arbeitsfehler der private Schlüssel beschädigt, unbrauchbar, versehentlich gelöscht wurde oder nicht mehr mit dem öffentlichen Schlüssel korrespondiert. Ohne den privaten Schlüssel können keine Kryptofunktionen (Signatur, Verschlüsselung) durchgeführt werden. Somit ist auch das Zertifikat unbrauchbar.

Unter diesen Voraussetzungen kann ein Zertifikat-Re-Issue basierend auf den aktuellen Identifikationsdaten und mit dem gleichen Zertifikatsinhalt beauftragt werden. Auf Basis des gleichen Subject-DN (Kapitel 3.1.1.1) wird ein neues Zertifikat generiert, das eine neue Seriennummer, ein neues Ausstellungsdatum aber das Ablaufdatum des Vorgängerzertifikats besitzt. Es empfiehlt sich, ein neues Schlüsselpaar zu generieren und den neuen öffentlichen Schlüssel zu verwenden. Die Sperrung des nicht mehr verwendeten Zertifikats ist durch den Kunden umgehend nach Aktivierung des neuen Zertifikats durchzuführen.

Bei der Verwendung des gleichen Schlüsselpaares wird vorausgesetzt, dass die eindeutige Zuordnung von Zertifikatsnehmer und Schlüssel gewährleistet ist, keine Kompromittierung des Schlüssels vorliegt und die kryptografischen Verfahren (z.B. Schlüssellänge) für die Gültigkeitsdauer des neuen Zertifikats noch ausreichend sind.

Ob Zertifikat-Re-Issue für die verwendete Anwendung möglich ist und ob ein neues Schlüsselpaar und damit der „neue“ öffentliche Schlüssel verwendet werden kann, hängt von

den technischen Vorgaben der Anwendung (z.B. Webserver) ab und obliegt der Verantwortung des Kunden.

4.7.8.2 TeleSec ServerPass EV/EV SAN:

Das Re-Issue entspricht dem bei ServerPass Standard und SAN/UCC. Einzige Ausnahme: Es muss immer ein neues Schlüsselpaar verwendet werden.

4.7.9 Bedingungen für ein Re-Issue

Ein Zertifikat-Re-Issue ist jederzeit während der Laufzeit des aktuellen Zertifikats möglich. Ein Zertifikat-Re-Issue eines gesperrten, ungültigen oder abgelaufenen Zertifikats ist nicht möglich. Das Ursprungszertifikat, das durch Re-Issue wieder ausgestellt wurde, kann nicht noch einmal die Option Re-Issue verwenden. Das nicht mehr benötigte Zertifikat ist umgehend vom Kunden zu sperren.

Das System überwacht, ob das Zertifikat durch den Kunden gesperrt wird. Nach 30 Tagen wird eine Zwangssperrung durchgeführt.

4.7.10 Wer darf eine Re-Issue beauftragen?

Das Zertifikat-Re-Issue wird ausschließlich von registrierten und autorisierten Personen beauftragt. Die autorisierte Person verfügt sowohl über die erforderlichen Login-Daten als auch über das Zertifikat-Service-Passwort.

4.7.11 Bearbeitung von Re-Issue Vorgängen

Die Beauftragung für ein Re-Issue wird elektronisch geprüft und kann, nach erfolgreicher Prüfung aller relevanten Daten, freigegeben werden. Im Zuge dieser Beauftragung muss der Auftraggeber den aktuell gültigen Vertragsbedingungen (z.B. AGB, Leistungsbeschreibung, Nutzungsbedingungen, etc.) zustimmen.

4.7.12 Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines Re-Issue Zertifikats

Es gelten die Regelungen gemäß Kapitel 4.3.2.

4.7.13 Annahme des Re-Issue

4.7.13.1 TeleSec ServerPass Standard und SAN/UCC:

Es gelten die Regelungen gemäß Kapitel 4.4.1.

4.7.13.2 TeleSec ServerPass EV/ EV SAN:

Re-Issue wird derzeit nicht angeboten.

4.7.14 Veröffentlichung des Re-Issue durch die CA

Es gelten die Regelungen gemäß Kapitel 4.4.2.

4.7.15 Benachrichtigung weiterer Stellen über ein Re-Issue durch die CA

Es gelten die Regelungen gemäß Kapitel 4.4.3.

4.8 Änderung von Zertifikatsdaten

Wenn sich Zertifikatsdaten im vorhandenen Zertifikat ändern, dann muss das Zertifikat neu beauftragt werden.

4.8.1 Bedingungen für eine Zertifikatsänderung

Das Ausstellen eines neuen Zertifikats ist zwingend erforderlich, wenn sich Zertifikatsinhalte (außer öffentlicher Schlüssel) ändern bzw. geändert haben.

4.8.2 Wer darf eine Zertifikatsänderung beauftragen?

Nicht anwendbar.

4.8.3 Bearbeitung von Zertifikatsänderungen

Nicht anwendbar.

4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines Zertifikats

Nicht anwendbar.

4.8.5 Annahme einer Zertifikatsänderung

Nicht anwendbar.

4.8.6 Veröffentlichung eines Zertifikats mit geänderten Daten durch die CA

Nicht anwendbar.

4.8.7 Benachrichtigung weiterer Stellen durch die CA über eine Zertifikatsausstellung

Nicht anwendbar.

4.9 Zertifikatssperrung und Suspendierung

4.9.1 Umstände für eine Sperrung

4.9.1.1 Gründe für die Sperrung eines Endteilnehmer-Zertifikats

Die folgenden Gründe erfordern die Zertifikatssperrung durch den Zertifikatsnehmer:

- der private Schlüssel wurde kompromittiert, verloren, gestohlen oder offen gelegt oder es besteht ein dringender Verdacht, dass dies geschehen ist,
- die Angaben im Zertifikat (mit Ausnahme nicht verifizierter Endteilnehmer-Informationen) sind nicht mehr aktuell, ungültig, falsch oder entsprechen nicht den Bestimmungen der Namensgebung (siehe Kapitel 3.1 ff.). Dies gilt auch für Domainnamen, die nicht mehr im Besitz des Domaininhabers sind oder die von befugten Instanzen (z.B. ICANN) zurückgezogen wurden (z.B. generische Top-Level-Domains (gTLD),
- die vormals interne Top-Level-Domain wird zu einer öffentlichen Top-Level-Domain (Kollision der Domainnamen),

- der zertifizierte Schlüssel (öffentliche Schlüssel) oder die damit verwendeten kryptografischen Algorithmen und Parameter entsprechen nicht mehr den aktuellen Anforderungen,
- es liegt ein Missbrauch oder Verdacht auf Missbrauch durch zur Nutzung des Schlüssels berechtigte Personen vor,
- gesetzliche Vorschriften oder richterliche Urteile,
- das Zertifikat wird nicht mehr benötigt bzw. der Zertifikatnehmer verlangt ausdrücklich die Sperrung des Zertifikats.

Die Zertifizierungsstelle sperrt ein Zertifikat innerhalb von 24 Stunden, wenn mindestens einer der folgenden Gründe vorliegt:

- Der Zertifikatsnehmer oder Bevollmächtigte reicht der Zertifizierungsstelle den Auftrag zur Sperrung schriftlich ein,
- Der Zertifikatsnehmer oder Bevollmächtigte informiert die Zertifizierungsstelle darüber, dass der zugrundeliegende Zertifikatsrequest nicht autorisiert war und die Autorisierung auch nachträglich nicht gegeben wird
- Der Zertifizierungsstelle liegen Beweise vor, dass der private Schlüssel des Zertifikatsnehmers kompromittiert wurde.
- Die Zertifizierungsstelle erlangt Kenntnis darüber, dass dem Nachweis der Domainkontrolle für einen FQDN oder eine IP-Adresse nicht vertraut werden kann.
- Die Zertifizierungsstelle erlangt Kenntnis davon, dass es eine Methode gibt, mit der der man den zu einem öffentlichen Schlüssel korrespondierenden privaten Schlüssel einfach berechnen kann. (vergleichbar mit der Debian Schwäche, Debian weak key, http://wiki.debian.org).

Ein Endteilnehmer-Zertifikat wird, wenn möglich innerhalb von 24 Stunden aber spätestens innerhalb von fünf Tagen gesperrt, wenn einer der folgenden Sperrgründe vorliegt.

- Das Zertifikat entspricht nicht mehr den Anforderungen aus Kapitel 6.1.5 und Kapitel 6.1.6.
- Der Zertifizierungsstelle liegen Beweise vor, dass das Zertifikat missbräuchlich eingesetzt wurde.
- Die Zertifizierungsstelle erlangt Kenntnis von einer oder mehreren schwerwiegenden Vertragsverletzungen des Zertifikatsnehmers.
- Die Zertifizierungsstelle erlangt Kenntnis darüber, dass das Nutzungsrecht für einen FQDN oder eine IP-Adresse erloschen ist. (Z.B. ein Gericht untersagt die Nutzung, eine Vollmacht läuft aus usw.)
- Die Zertifizierungsstelle erlangt Kenntnis, dass ein Wildcard-Zertifikat für die Authentisierung eines missverständlichen untergeordneten FQDN, der betrügerisch verwendet wird.
- Die Zertifizierungsstelle erlangt Kenntnis von einer relevanten Änderung in den Zertifikatseinträgen.
- Die Zertifizierungsstelle erhält Kenntnis davon, dass das Zertifikat nicht regelkonform herausgegeben wurde, wie es in den Anforderungen des CA-Browserforums oder der anzuwendenden CP oder CPS beschrieben ist.
- Die Zertifizierungsstelle stellt fest, dass eine Information im Zertifikat nicht korrekt oder missverständlich ist.
- Die Zertifizierungsstelle stellt den Betrieb ein und hat keine Regelungen getroffen, dass im Falle einer Betriebseinstellung der Sperrsupport durch eine andere CA weitergeführt wird.
- Der Nachweis der CA-Browserforum-Konformität der CA hat seine Gültigkeit verloren. Ein Sperrgebot gilt nicht, wenn die Zertifizierungsstelle Vorsorge getroffen hat, dass die CRL und der OCSP-Dienst weiter gepflegt und bereitgestellt werden.

- Der Root TSP sieht eine Sperrung vor.
- Die Inhalte oder das Format des Zertifikats stellt aus technischer Sicht ein inakzeptables Risiko für Anwendungssoftware-Hersteller oder vertrauende Dritte dar z.B. wenn das CA-Browserforum ein solches Risiko aufzeigt und deshalb das Zertifikat gesperrt und ersetzt werden sollte.
- Gesetzliche Vorschriften oder richterliche Urteile oder eine Weisung einer aufsichtsführenden Behörde liegt vor.

4.9.1.1.1 TeleSec ServerPass EV/EV SAN:

Zusätzlich zu diesen Gründen gibt es noch eine Reihe spezifische Gründe, welche in [CABF-BREV] genannt werden und von der Zertifizierungsstelle entsprechend erfasst und protokolliert werden:

- Das EV/EV SAN-Zertifikat ist nicht autorisiert. Das heißt, dass zum Beispiel nachträglich festgestellt wird, dass die Ausgabe des EV/EV SAN-Zertifikats unter falschen Voraussetzungen stattgefunden hat.
- Die Nutzungsbedingungen wurden missachtet.
- Das Zertifikat widerspricht den Bestimmungen und Bedingungen zur Ausstellung von EV-Zertifikaten.

4.9.1.2 Gründe für die Sperrung eines Sub-CA-Zertifikats

Die Zertifizierungsstelle veranlasst die Sperrung eines Sub-CA-Zertifikat, wenn

- der ursprüngliche Zertifikatsantrag nicht autorisiert war und auch nicht rückwirkend autorisiert werden kann oder soll,
- der private Schlüssel der Sub-CA kompromittiert oder einer nicht autorisierten Person oder einer Organisation, die nicht mit der Sub-CA verbunden ist, bekannt gegeben wurde oder nicht mehr den Anforderungen (siehe Kap. 6.1.5 und 6.1.6) entspricht,
- das Zertifikat missbräuchlich eingesetzt wurde,
- das Sub-CA-Zertifikat nicht konform zur Trust Center CP herausgegeben wurde oder der TSP nicht konform zur Trust Center CP arbeitet,
- eine Information im Zertifikat nicht korrekt oder missverständlich ist,
- der Betrieb der Sub-CA eingestellt wird und keine Regelungen zur Weiterführung des Sperrservice getroffen wurden,
- das Recht der Sub-CA, Zertifikate gemäß den Anforderungen der Trust Center CP auszustellen erlischt oder widerrufen oder beendet wird und keine Vorkehrungen zum weiteren Betrieb der Sperrservices getroffen wurden.

Darüber hinaus kann die Zertifizierungsstelle die Sperrung eines Sub-CA-Zertifikats ohne Angabe von Gründen beantragen.

4.9.2 Wer kann eine Sperrung beauftragen?

Die folgenden Personen und Institutionen sind berechtigt, die Sperrung eines Zertifikates zu initiieren:

- autorisierte Personen in Vertretung für juristische Personen.
- Registrierungsmitarbeiter des Trust Centers.

Insbesondere gelten die Regelungen aus Kapitel 3.4.1.

4.9.3 Ablauf einer Sperrung

4.9.3.1 Sperrung von Endteilnehmer-Zertifikaten

Die Sperrung eines Zertifikats erfolgt in der Regel durch den Endteilnehmer 7x24h im Serviceportal <myServerPass> über den Aktionsbutton <Sperren>. Die Sperrung wird durch das Service-Passwort autorisiert und ist endgültig. Der Zertifikatsnehmer wird automatisch per E-Mail über den Sperrstatus informiert.

Das Trust Center behält sich jederzeit (7x24h) vor, Zertifikate bei Vorliegen von mindestens einem, der in Kapitel 4.9.1.1 aufgeführten Sperrgründe, zu sperren.

Das Trust Center bietet Anwendern, Usern, Softwareherstellern und anderen Dritten eine Möglichkeit an, verdächtige Schlüsselkompromittierungen, Zertifikatsmissbrauch oder andere zertifikatsbetreffende Betrugsfälle oder -versuche zu melden.

Innerhalb von 24 Stunden nach Eingang eines Missbrauchsverdachts beginnt das Trust Center mit den Nachforschungen, um entscheiden zu können, ob weitere Maßnahmen (zum Beispiel Sperrung) eingeleitet werden. Innerhalb dieser 24 Stunden wird ein erster Bericht des Sachverhalts und der Analyseergebnisse erstellt und dem Zertifikatsnehmer sowie der Person, die das Problem gemeldet hat, als Rückmeldung gegeben. Nach Ansicht der Fakten und Umgebungsparameter wird die Zertifizierungsstelle mit dem Zertifikatsnehmer/Beauftragten oder der meldenden Person die Analyseergebnisse besprechen und entscheiden, inwiefern eine Zertifikatssperrung notwendig wird. In diesem Zusammenhang wird das Datum der Sperrung festgelegt.

Der Zeitraum zwischen Erhalt des Zertifikatsproblemreports bzw. Sperrwunsches bis zur veröffentlichten Sperrung darf die in Kapitel 4.9 geforderten Fristen für eine Sperrung nicht überschreiten.

Das weitere Vorgehen wird anhand folgender Kriterien bestimmt:

- Die Ursache oder Art des Problems (Kontext, Schwere, Auswirkungen, Risiko oder Schaden)
- Die Auswirkungen einer Sperrung (direkte oder gemeinsame Auswirkungen auf Zertifikatsinhaber und vertrauende Dritte)
- Die Anzahl der Meldungen zu diesem Zertifikatsproblem oder von diesem Zertifikatsinhaber
- Die Entität, welche die Meldung eingestellt hat (z.B. eine Meldung durch eine Strafverfolgungsbehörde wird mit erhöhter Priorität eingestuft) und
- Die bezugnehmende Gesetzgebung

Das Trust Center verfügt bei einer hoch priorisierten Zertifikats-Problemmeldung jederzeit über die Möglichkeit intern zu reagieren und zu entscheiden, ob eine Weiterleitung an eine Strafverfolgungsbehörde erforderlich ist oder ein Zertifikat, das Gegenstand einer solchen Meldung ist, zu sperren.

4.9.4 Fristen für einen Sperrauftrag

Sobald ein Sperrgrund gemäß Kapitel 4.9.1.1 vorliegt, muss der Sperrauftrag so schnell wie möglich innerhalb einer wirtschaftlich angemessenen Frist gestellt werden.

4.9.5 Fristen für die Bearbeitung eines Sperrauftrags durch die CA

Die Sperroption steht dem Endteilnehmer 7x24h zur Verfügung und wird unmittelbar nach dem Sperrvorgang im Serviceportal <myServerPass> an die angeschlossenen Systeme

weitergegeben. Der OCSP-Service, der auf diese Systeme zugreift, verfügt damit ebenfalls über den aktuellen Zertifikatsstatus.

Der Zeitraum zwischen Erhalt des Sperrantrags bis zur veröffentlichten Sperrung darf die in Kapitel 4.9 geforderten Fristen für eine Sperrung nicht überschreiten.

4.9.6 Überprüfungsmethoden für Vertrauende Dritte

Vertrauende Dritte müssen die Möglichkeit erhalten, den Status von Zertifikaten überprüfen zu können, denen sie vertrauen möchten.

Zu diesem Zweck kann der OCSP Service genutzt werden, der den aktuellen Status eines Server-Zertifikats anzeigt. Eine weitere Methode, wie ein Vertrauender Dritter überprüfen kann, ob ein Zertifikat gesperrt ist, ist die Prüfung der aktuellen Zertifikatssperrliste (CRL), die im Verzeichnisdienst veröffentlicht wird.

Die Sperrlisten enthalten auch abgelaufene Zertifikate (ExpiredCertsOnCRL).

4.9.7 Frequenz der Veröffentlichung von Sperrinformationen

Die Zertifikatssperrliste (CRL) wird, wie in Kapitel 2.3 beschrieben, über den Verzeichnisdienst publiziert.

Die Zertifikatssperrliste (CRL), in der gesperrte Zertifikate von Endteilnehmern aufgeführt sind, wird mindestens einmal pro Tag oder anlassbezogen aktualisiert und über den Verzeichnisdienst veröffentlicht. Regelmäßig eingeplante CRLs werden vor dem Zeitpunkt ausgegeben, der im Feld nextUpdate der zuvor ausgegebenen CRL hinterlegt ist.

Vor der Außerbetriebnahme einer Sub-CA wird eine letzte CRL mit einem nextUpdate-Wert erstellt, der nach dem Zeitpunkt des notAfter-Werts des zugehörigen CA-Zertifikats liegt. Diese CRL wird bis zu dem auf den Ablauf des ausstellenden CA-Zertifikats folgenden Tag bereitgestellt.

4.9.8 Maximale Latenzzeit von Sperrlisten

Die Latenzzeit der Zertifikatssperrliste (CRL) nach automatischer Generierung beträgt wenige Minuten. Die Latenzzeit für Zertifizierungsstellen-Sperrliste (CARL/ARL) nach manueller Veröffentlichung beträgt wenige Minuten.

4.9.9 Online-Verfügbarkeit von Sperr-/Statusinformationen

Zusätzlich, zu den Sperrinformationen über CRL und CARL/ARL stellt die Zertifizierungsstelle Online-Informationen zum Zertifikatsstatus via OCSP bereit. OCSP-Antworten für von ServerPass ausgestellte Endteilnehmer-Zertifikate entsprechen den Vorgaben aus RFC 6960.

Die URL des OCSP-Responders ist im Zertifikat in der Erweiterung „Zugriff auf Stelleninformation (Authority Information Access)“ (siehe Kapitel 7.1.2.9) aufgeführt.

4.9.10 Anforderungen an Online-Überprüfungsverfahren

Vertrauende Dritte müssen den Status eines Zertifikats überprüfen, um Informationen darüber zu erhalten, ob ein Zertifikat, dem sie vertrauen möchten, vertrauenswürdig ist. Für den Abruf aktueller Statusinformationen steht der OCSP-Service (OCSP-Responder) zur Verfügung.

Die ausgegebenen OCSP-Antworten von Endteilnehmer-Zertifikaten entsprechen den Vorgaben des RFC 6960.

Der OCSP-Responder antwortet auf Anfragen nach nicht vom Dienst TeleSec ServerPass ausgestellten Zertifikats-Seriennummern mit „unknown“. Des Weiteren erfolgt ein Monitoring des OCSP-Responders auf Anfragen zu "nicht genutzten" Zertifikats-Seriennummern.

Der OSCP-Responder unterstützt die HTTP GET-Methode. Die OCSP-Datenquelle (repository) wird alle 10 Minuten synchronisiert. Die OCSP-Antworten sind 5 Tage gültig. Eine weitere Möglichkeit der Statusabfrage liefert die aktuelle Zertifikatssperrliste (CRL).

4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Der technische Ansprechpartner wird per E-Mail über die Sperrung des Zertifikats benachrichtigt (revoke notification), in der die relevanten Zertifikats-Informationen enthalten sind.

4.9.12 Besondere Anforderungen bezüglich der Kompromittierung privater Schlüssel

Bei einer Kompromittierung eines privaten Schlüssels ist das entsprechende Zertifikat unverzüglich zu sperren.

Dritte, die eine Schlüsselkompromittierung melden wollen, werden gebeten, die in Kap. Kontaktinformationen1.5.2 beschriebenen Kontaktmöglichkeiten zu nutzen. Es müssen ausreichende Informationen oder Verweise auf Informationen angegeben werden, die das Vorliegen einer Schlüsselkompromittierung beweisen, z. B. ein mit dem kompromittierten privaten Schlüssel signierter CSR mit commonName "Compromised Key". Das betroffene Zertifikat selbst sollte ebenfalls referenziert werden.

4.9.13 Suspendierung von Zertifikaten

Die Suspendierung (temporäre Sperrung) von Zertifikaten ist nicht vorgesehen.

4.9.14 Wer kann eine Suspendierung beauftragen?

Nicht anwendbar.

4.9.15 Verfahren der Suspendierung

Nicht anwendbar.

4.9.16 Beschränkung des Suspendierungszeitraums

Nicht anwendbar.

4.10 Statusauskunftsdienste für Zertifikate

Der Status von Endteilnehmer-Zertifikaten kann durch den OCSP-Service angezeigt werden. Außerdem können gesperrte Zertifikate durch die Zertifikatssperrliste (CRL) ermittelt werden.

4.10.1 Betriebseigenschaften

OCSP-Antworten werden von einem OCSP-Responder signiert, dessen Zertifikat seinerseits von der ServerPass Sub-CA signiert wurde, welche das betreffende Endteilnehmer-Zertifikat ausgestellt hat.

Das Zertifikat des OCSP-Responders enthält die in Kapitel 7.3.1 beschriebene Erweiterung.

Die OCSP-Antwort enthält einen der folgenden Stati:

- gut (good) bedeutet:
  - es ist ein Aussteller /Issuer des Services und
  - das Zertifikat ist gültig (innerhalb der Zertifikatslaufzeit) und
  - das Zertifikat ist nicht gesperrt.
- gesperrt (revoked) bedeutet:
  - es ist ein Aussteller/Issuer des Services und
  - das Zertifikat ist gültig (innerhalb der Zertifikatslaufzeit) und
  - das Zertifikat wurde gesperrt.
- unbekannt (unknown) bedeutet:
  - das Zertifikat ist ungültig (außerhalb der Zertifikatslaufzeit) oder
  - das Zertifikat ist gültig, wurde aber nicht von dem angefragten Aussteller/Issuer des Services ausgestellt oder
  - das Zertifikat ist gültig, wurde aber nicht von dem Aussteller/Issuer des Services ausgestellt.

Die Zertifizierungsstelle hat Mechanismen zum Schutz des Sperrstatus-Dienstes (CRL, ARL, OCSP) gegen unbefugte Versuche implementiert, um Manipulationen an Sperrstatusinformationen (hinzufügen, löschen, ändern) zu verhindern.

OCSP-Stapling wird nicht angeboten.

4.10.2 Verfügbarkeit des Dienstes

Der Zertifikatsstatus-Service steht 7x24h zur Verfügung. Die Antwortzeit des OCSP-Responders beträgt unter normalen Betriebsbedingungen weniger als 3 Sekunden.

Es sind Maßnahmen getroffen, die in der Regel einen Betrieb der OCSP-Responder ohne Downtime gewährleisten (mehrfache Redundanzen, Caching). In Notfallszenarien sind Downtimes von bis zu einem Tag möglich.

Die Sperrinformationen für Endteilnehmerzertifikate werden bis zu dem auf den Ablauf des ausstellenden CA-Zertifikats folgenden Tag bereitgestellt.

4.10.3 Weitere Merkmale

Nicht anwendbar.

4.11 Beendigung der Zertifikatsnutzung

Bei Beendigung der Zertifikatsnutzung vor Ablauf der Gültigkeit muss das Zertifikat durch den Endteilnehmer gesperrt werden.

4.12 Schlüsselhinterlegung und Wiederherstellung

4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

Für die im Trust Center betriebene Zertifizierungsstelle TeleSec ServerPass wird das Schlüsselpaar auf einem sicherheitsüberprüften Hardware Security Module (HSM) hinterlegt und in sicherer Umgebung abgelegt. Die Speicherung des Schlüsselmaterials auf weiteren HSM erfolgt ausschließlich zur Schlüsselhinterlegung (Back-Up) und dient zu Wiederherstellung und Aufrechterhaltung des Dienstes durch qualifiziertes Personal (Trusted Role) des Trust Centers. Eine Schlüsselhinterlegung bei Dritten (z.B. Treuhänder, Notar) ist nicht realisiert.

4.12.2 Richtlinien und Praktiken zum Schutz und Wiederherstellung von Sitzungsschlüsseln

Nicht anwendbar.

5 PHYSIKALISCHE, ORGANISATORISCHE UND PERSONELLE SICHERHEITSMAßNAHMEN

Das Trust Center der Deutschen Telekom Security GmbH liegt im Geltungsbereich einer vom Management freigegebenen Sicherheitsleitlinie und einem dazu gehörigen Informationssicherheitsmanagementsystem (ISMS), welches nach ISO 27001 zertifiziert ist.

Das ISMS selbst sowie weitere Sicherheitsrichtlinien, Sicherheitskonzepte und andere Dokumente stellen die Einhaltung der in der Telekom Security CP (Kapitel 5) genannten Anforderungen sicher. Insbesondere umfasst das Risikomanagement eine Risikoanalyse unter Einbeziehung von Eintrittswahrscheinlichkeiten und Schadensausmaßen sowie einer angemessenen Risikobehandlung inkl. einer abschließenden (Rest-)Risikoakzeptanz. Die Prozesse des Risikomanagements werden mindestens jährlich sowie anlassbezogen durchgeführt.

5.1 Physikalische Maßnahmen

Anlagen, Medien und Informationen des Trust Centers werden entsprechend ihrer Kritikalität durch physikalische Maßnahmen vor Verlust, Diebstahl, Schaden oder Kompromittierung geschützt. Diese Maßnahmen sind in internen Sicherheitskonzepten und weiteren Dokumenten festgehalten.

5.1.1 Standort und Bauweise

Die Infrastruktur des Trust Centers befindet sich in zwei georedundanten Rechenzentren (ein sogenanntes Twin-Core Rechenzentrum) innerhalb Deutschlands. Bei der Wahl der Standorte wurden, basierend auf einer entsprechenden Risikoanalyse, die umgebungsbezogenen Gegebenheiten wie die Anfälligkeit für Naturkatastrophen und andere Gefahrenquellen berücksichtigt. Die Bauweise und Infrastruktur des Gebäudes ist für den sicheren Betrieb kritischer Systeme ausgelegt und erfüllt die Anforderungen an eine Hochsicherheitszone.

Die für den Betrieb des Trust Centers relevanten Bereiche sind durch zusätzliche Einhausungen von allen anderen Bereichen getrennt und nach „Trusted Site Infrastructure TSI V3.2 Dual Site“ auditiert und zertifiziert.

5.1.2 Physikalischer Zutritt

Die Rechenzentren verfügen über umfängliche physische Sicherheitsmaßnahmen, die unter anderem Sicherheitspersonal, gesicherte Eingänge, Einbruchmeldeanlagen und Multi-Level-Zugangssysteme umfassen. Insbesondere sind die Räumlichkeiten des Trust Centers ausschließlich für berechtigte Personen in vertrauenswürdigen Rollen zugänglich und Besucher nur in Begleitung einer solchen Person gestattet. Die Zutrittsrechte werden regelmäßig sowie bei Bedarf überprüft und ggf. angepasst.

5.1.3 Stromversorgung und Klimatisierung

Die Rechenzentren sind mit redundanten Stromversorgungen und Klimaanlagen ausgestattet. Die Systeme werden vor Spannungsschwankungen geschützt und sind durch unterbrechungsfreie Stromversorgungen (Kurz- und Langzeitüberbrückungen) mit Kreuz-Verkabelung abgesichert.

5.1.4 Wassereinwirkung

Die Rechenzentren befinden sich außerhalb des Gefahrenbereichs von Hochwasser oder anderen Gefahrenquellen. Darüber hinaus sind die Räumlichkeiten selbst durch weitere Maßnahmen vor Wassereinbruch bzw. Wasserschäden geschützt.

5.1.5 Brandvorsorge und Brandschutz

Die Rechenzentren sind dem kritischen Schutzbedarf entsprechend mit baulichen Maßnahmen und gemäß geltender Brandschutzbestimmungen vor Brandschäden geschützt.

5.1.6 Aufbewahrung von Medien

Medien werden ausschließlich in den Betriebsräumen des Trust Centers, vor Feuer- und Wassereinwirkung sowie unberechtigtem Zugriff geschützt, aufbewahrt. Es werden keine Medien zur dauerhaften oder langfristigen Speicherung oder Archivierung eingesetzt.

5.1.7 Abfallentsorgung

Vertrauliche Dokumente und Datenträger werden ausschließlich über zertifizierte Entsorgungsunternehmen sicher entsorgt. Alle Datenträger werden darüber hinaus vor ihrer Entsorgung mit zertifizierten Verfahren gelöscht.

5.1.8 Externe Sicherung

Keine Bestimmungen.

5.2 Organisatorische Maßnahmen

Die relevanten Anforderungen aus [ETSI EN 319 401] Kap. 7.4 b, c, d, e sind umgesetzt.

5.2.1 Vertrauenswürdige Rollen

Der TSP ist auf Basis der folgenden vertrauenswürdigen Rollen organisiert:

- Leiter TSP: trägt die gesamte Verantwortung für die bereitgestellten Dienste des Trust Centers
- Informationssicherheitsbeauftragter: plant und überwacht die Implementierung von Sicherheitsmaßnahmen, verantwortet Schwachstellenscans und Penetrationstests, leitet das ISMS
- ISMS-Teammitglied: unterstützt den Informationssicherheitsbeauftragten in seinen Aufgaben
- Administrator: konfiguriert und wartet die IT-Infrastruktur (Netzwerke, Datenbanken, Server und richtet technisch die Zugriffsrechte für die Mitarbeiter der RA ein, etc.)
- CA Operator: generiert CA-Schlüssel und importiert die erstellten CA-Zertifikate.
- Interner Auditor: prüft regelmäßig sowie bei Unstimmigkeiten Zertifikate, Prozesse, Dokumentationen und begutachtet die Konformität von Schlüssel- bzw. Root-Zeremonien
- Root-Programm/Compliance-Team (PKI): koordiniert die Umsetzung von Anforderungen, überwacht Anforderungsquellen (Mailing-Listen, Root-Store-Policies, ETSI), übernimmt Außenkommunikation zu Root-Store-Betreibern und „Bugzilla“, berät bei Vorfällen und Änderungen, verantwortet CP, bearbeitet Anträge für CA-Ausstellungen
- Auftragsbearbeiter (RAOP): Bearbeitung von Zertifikatsaufträgen
- Kryptobeauftragter: Experte für kryptografische Themen
- Produktmanager: Verantwortung für das Lifecyclemanagement des TSP

- Technischer Produktmanager: Anforderungsmanagement und Produkttests

Die oben genannten vertrauenswürdigen Personen müssen die in diesem CPS festgelegten Anforderungen (siehe Kapitel 5.3.1) erfüllen.

5.2.2 Anzahl der für eine Aufgabe erforderlichen Personen

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

Es sind technische und organisatorische Maßnahmen etabliert, wodurch sicherheitsrelevante oder -kritische Tätigkeiten nur durch Personen in vertrauenswürdigen Rollen und nur im Vier-Augen-Prinzip durchgeführt werden. Die Anzahl der Mitarbeiter, die solche sicherheitsrelevanten oder -kritischen Tätigkeiten ausüben, ist unter Berücksichtigung von Vertreterregelungen und arbeitstechnischen Umständen auf ein Minimum beschränkt.

TeleSec ServerPass EV/EV SAN:

Das in den EV Guidelines [CABF-BREV] geforderte Vier-Augen-Prinzip im Genehmigungsprozess eines EV/EV SAN-Zertifikats wird von der Zertifizierungsstelle entsprechend den Anforderungen umgesetzt. Eine Umgehung des Vier-Augen-Prinzips wird mit technischen Mitteln unterbunden.

Die Prüfung der SubjectDN-Angaben erfolgt darüber hinaus für jeden Auftrag in Vier-Augen-Prinzip.

5.2.3 Identifizierung und Authentifizierung für jede Rolle

Die Identifizierung geeigneter Personen zur Besetzung von Rollen, die Übertragung der Rollen (Authentifizierung) sowie deren Entzug erfolgen nach einem dokumentierten Prozess, welcher u.a. die Klärung des Bedarfs bzw. Ausschluss von Interessenskonflikten, die Bereitschaft der Person zur Übernahme der Tätigkeiten, die Freigabe durch die Führungskraft und die Dokumentation von Nachweisen hierfür beinhalten.

Vor der Übertragung einer vertrauenswürdigen Rolle (oder schon bei der Einstellung als Mitarbeiter) wird die entsprechende Person unter Vorlage eines amtlichen Ausweises persönlich identifiziert und es werden von dieser Person sowie der Leitung des Trust Centers die Akzeptanz zur Übertragung der Rolle, der damit verbundenen Verantwortung und den daraus resultierenden Pflichten zur Gewährleistung der Sicherheit eingeholt.

Rollen werden nur an Personen übertragen, wenn dadurch keine Interessenskonflikte (siehe dazu auch Kapitel 5.2.1 und 5.2.4) entstehen und die Unabhängigkeit gewahrt wird, d.h. dass

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

Diese Struktur, die die Unparteilichkeit des Betriebs gewährleistet, ist unter anderem im ISMS-Handbuch des Trust Centers dokumentiert.

Die Rolleninhaber werden offiziell von der Leitung des Trust Centers in die vertrauenswürdige Rolle berufen.

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

Die Vergabe der erforderlichen Berechtigungen erfolgt nach dem „Least Privilege“-Prinzip, d.h. alle Berechtigungen sind auf das erforderliche Minimum beschränkt.

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

5.2.4 Rollen, die eine Aufgabentrennung erfordern

Es sind folgende Rollen voneinander getrennt:

- Management des TSP,
- IT-Sicherheitsbeauftragter und/oder interner Auditor,
- RAOP und
- Administrator und/oder CA-Operator.

Zur Vermeidung von Interessenskonflikten müssen der TSP und der Antragsteller unterschiedliche Entitäten sein. Als einzige Ausnahme gilt der TSP selbst, wenn dieser TLS-Zertifikate für eigene Server beauftragt.

5.3 Personelle Maßnahmen

Das Trust Center setzt umfassende personelle Sicherheitsmaßnahmen um, die einen hohen Schutz ihrer Einrichtungen und der Zertifizierungsdienste gewährleisten. Im Trust Center ist der Einsatz von qualifiziertem geschultem Personal obligatorisch die personellen Maßnahmen sind im Sicherheitskonzept niedergelegt.

5.3.1 Anforderungen an Qualifikation, Erfahrung und Sicherheitsüberprüfung

Das Trust Center verlangt von seinen Mitarbeitern, die eine vertrauenswürdige Rolle einnehmen sollen, entsprechende Nachweise über Qualifizierung und Erfahrung, die dazu notwendig sind, ihre voraussichtlichen beruflichen Pflichten kompetent und zufriedenstellend zu erfüllen.

In regelmäßigen Abständen ist dem Personalvorgesetzten ein neues Führungszeugnis vorzulegen.

5.3.2 Sicherheitsüberprüfung

Vor dem Beginn der Beschäftigung in einer vertrauenswürdigen Rolle führt das Trust Center eine Sicherheitsüberprüfung durch mit folgendem Inhalt durch:

- Überprüfung und Bestätigung der bisherigen Beschäftigungsverhältnisse,
- Überprüfung von Arbeitszeugnissen,
- Bestätigung des höchsten oder maßgebenden Schul-/Berufsabschlusses,
- polizeiliches Führungszeugnis.

Sofern die in diesem Abschnitt festgelegten Anforderungen nicht erfüllt werden können, macht das Trust Center ersatzweise Gebrauch von einer gesetzlich zulässigen Ermittlungsmethode, die im Wesentlichen die gleichen Informationen liefert.

Ergebnisse einer Sicherheitsüberprüfung, die zu einer Ablehnung eines Anwärters für eine vertrauenswürdige Person führt, können beispielsweise sein

- falsche Angaben seitens des Anwärters oder der vertrauenswürdigen Person,

- besonders negative oder unzuverlässige berufliche Referenzen, und
- gewisse Vorstrafen.

Berichte, die solche Informationen enthalten, werden durch Mitarbeiter der Personalabteilung und Sicherheitspersonal bewertet, die das weitere angemessene Vorgehen festlegen. Das weitere Vorgehen kann Maßnahmen bis einschließlich zur Rücknahme des Einstellungsangebots an Anwärter für vertrauenswürdige Positionen führen oder der Kündigung von vertrauenswürdigen Personen beinhalten.

Die Verwendung von in einer Sicherheitsüberprüfung ermittelten Informationen zur Ergreifung solcher Maßnahmen unterliegt geltendem Recht.

5.3.3 Schulungs- und Fortbildungsanforderungen

Das Personal des Trust Centers besucht Fortbildungsmaßnahmen die zur kompetenten und zufriedenstellenden Erfüllung ihrer beruflichen Pflichten erforderlich sind. Das Trust Center führt Unterlagen über diese Schulungsmaßnahmen.

Die Schulungsprogramme sind auf die individuellen Tätigkeitsbereiche abgestimmt und beinhalten u.a.:

- fortgeschrittene PKI-Kenntnisse,
- Verfahrensweisen nach ITIL,
- Datenschutz,
- Daten- und Fernmeldegeheimnis,
- Informationsschutz,
- Zutrittsschutz,
- Antikorruption,
- Sicherheits- und Betriebsrichtlinien und –verfahren des DTAG-Konzerns,
- Verwendung und Betrieb eingesetzter Hardware und Software,
- Meldung von und Umgang mit Störungen und Kompromittierungen und
- Verfahren für die Schadensbehebung im Notfall (Disaster Recovery) und Geschäftskontinuität (Business Continuity).

Mitarbeiter, welche mit der Validierung von Zertifikatsaufträgen befasst sind, erhalten zusätzlich Schulungen in den folgenden Bereichen:

- Richtlinien, Verfahren und aktuelle Entwicklungen zu Validierungsmethoden,
- Inhalte und insbesondere relevante Änderungen des vorliegenden CPS und der zugehörigen CP,
- Relevante Anforderungen und Vorgaben aus den Zertifizierungsnormen,

Allgemeine Bedrohungs- und Angriffsszenarien bzgl. der Validierungsmethoden (z.B. Social Engineering).

5.3.4 Nachschulungsintervalle und -anforderungen

Das Personal des Trust Centers erhält im erforderlichen Umfang aber spätestens nach Ablauf von 12 Monaten Auffrischungsschulungen und Fortbildungslehrgänge. Die Erfordernisse werden jährlich überprüft und im Schulungsprogramm eingepflegt.

5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Nicht anwendbar.

5.3.6 Sanktionen bei unbefugten Handlungen

Die Zertifizierungsstelle behält sich vor, unbefugte Handlungen oder andere Verstöße gegen dieses CPS und der daraus abgeleiteten Verfahren zu ahnden und entsprechende Disziplinarmaßnahmen einzuleiten. Diese Disziplinarmaßnahmen können Maßnahmen bis einschließlich der Kündigung beinhalten und richten sich nach der Häufigkeit und Schwere der unbefugten Handlungen.

5.3.7 Anforderungen an unabhängige Auftragnehmer

Das Trust Center behält sich vor, unabhängige Auftragnehmer oder Berater zur Besetzung vertrauenswürdiger Positionen einzusetzen. Diese Personen unterliegen denselben Funktions- und Sicherheitskriterien wie Mitarbeiter des Trust Centers in vergleichbarer Position.

Obiger Personenkreis, der die in Kapitel 5.3.2 beschriebene Sicherheitsüberprüfung noch nicht abgeschlossen oder nicht erfolgreich durchlaufen hat, wird der Zugang zu den gesicherten Einrichtungen des Trust Centers nur unter der Bedingung gestattet, dass sie stets von vertrauenswürdigen Personen begleitet und unmittelbar beaufsichtigt werden.

5.3.8 Dokumentation für das Personal

Um die beruflichen Pflichten angemessen erfüllen zu können, stellt das Trust Center seinen Mitarbeitern alle dafür erforderliche Dokumente (Schulungsunterlagen, Verfahrensanweisungen) und Hilfsmittel zur Verfügung.

5.4 Protokollereignisse

Es ist im Loggingkonzept sowie im Installationshandbuch festgelegt, welche Daten und Ereignisse in welchen Abständen von wem aufgezeichnet werden. Darüber hinaus wird geregelt, wie lange die Protokolldaten gespeichert werden (aktuell 6 Wochen) und wie sie vor Verlust und unbefugtem Zugriff geschützt werden. Es werden dabei die Anforderungen aus [ETSI EN TSP] Kap. 7.10 umgesetzt.

5.4.1 Art der aufgezeichneten Ereignisse

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

5.4.1.1 CA-Schlüsselpaare und CA-Systeme

Für das Lifecycle--Management für CA-Schlüsselpaare bzw. von CA-Systemen protokolliert das Trust Center für TeleSec ServerPass mindestens die folgenden Ereignisse:

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

5.4.1.2 EE- und CA-Zertifikate

Für das Lifecycle-Management von EE- als auch CA-Zertifikaten protokolliert das Trust Center für TeleSec ServerPass mindestens die folgenden Ereignisse:

a) Erstauftrag und Sperrung von Zertifikaten

b) Auftrag zur Erneuerung mit und ohne Schlüsselwechsel (renewal und rekey)
c) Alle Tätigkeiten im Zusammenhang mit der Verifikation von Informationen
d) Das Ergebnis, sowie Datum/Uhrzeit und Rufnummer von Telefonaten im Zusammenhang mit der Verifikation und Name des Gesprächspartners
e) Annahme oder Ablehnung von Zertifikatsaufträgen
f) Ausstellung eines Zertifikates
g) Erzeugung von Sperrlisten und OCSP-Einträgen

5.4.1.3 Sonstige sicherheitsrelevante Ereignisse

Zusätzlich werden vom Trust Center für den Betrieb der Infrastruktur TeleSec ServerPass alle sicherheitsrelevanten Ereignisse protokolliert. Das beinhaltet mindestens die folgenden Ereignisse:

a) Erfolgreiche und erfolglose Zugriffsversuche auf Systeme der PKI,
b) Durchgeführte Aktionen an und durch PKI- und sonstigen sicherheitsrelevanter Systeme,
c) Änderungen an Sicherheitsprofil,
d) Systemabstürze, Hardware-Ausfälle und andere Anomalien,
e) Firewall- und Router-Aktivitäten,
f) Zutritt und Verlassen von Einrichtungen des Trust Centers
g) Ergebnisse von Netzwerkprüfungen (Schwachstellenüberprüfungen)
h) Start und Beendigung des Protokollierungsprozesses

5.4.2 Bearbeitungsintervall der Protokolle

Die erstellten Audit-Protokolle/Logging-Dateien werden permanent auf wichtige sicherheits- und betriebsrelevante Ereignisse untersucht. Ferner überprüft das Trust Center die Audit-Protokolle/Logging-Dateien auf verdächtige und ungewöhnliche Aktivitäten, als Folge von Unregelmäßigkeiten und Störungen des Services TeleSec ServerPass.

Eingeleitete Maßnahmen, die als Reaktion aus der Auswertung von Audit-Protokollen/Logging-Dateien stammen, werden ebenfalls protokolliert.

5.4.3 Aufbewahrungszeitraum für Audit-Protokolle

Audit-Protokolle/History-Daten/Logging-Dateien werden nach Bearbeitung gemäß Kapitel 5.5.2 archiviert.

5.4.4 Schutz der Audit-Protokolle

Audit-Protokolle/ History-Daten/Logging-Dateien werden gegen unbefugten Zugriff geschützt.

5.4.5 Sicherungsverfahren für Audit-Protokolle

Eine inkrementelle Sicherung von Audit-Protokollen/ History-Daten/Logging-Dateien wird täglich durchgeführt.

5.4.6 Audit-Erfassungssystem (intern vs. extern)

Audit-Daten/ History-Daten/Logging-Dateien von Anwendungs-, Netzwerk- und Betriebssystemebene werden automatisch erzeugt und aufgezeichnet. Manuell erzeugte Audit-Daten werden von Trust Center-Mitarbeitern aufgezeichnet.

5.4.7 Benachrichtigung des Ereignis-auslösenden Subjekts

Ereignisse, die das Audit-Monitoringsystem erfasst, werden bewertet an das zuständige Trust Center Personal weitergeleitet. Ereignisse mit hoher Priorität werden unverzüglich auch außerhalb der Regelarbeitszeit an das Trust Center Personal weitergeleitet.

5.4.8 Schwachstellenbewertung

Nach jeder signifikanten System- oder Netzwerkänderung oder einer Aufforderung vom CA/Browserforum erfolgt innerhalb einer Woche, mindestens jedoch einmal je Kalenderquartal eine automatisierte Schwachstellenüberprüfung (Vulnerability-Scan). Mögliche Schwachstellen werden analysiert, bewertet und registriert. Basierend auf der Auswertung werden Maßnahmen festgelegt und in einem definierten Plan umgesetzt. Die Schwachstellenüberprüfungen, ihre Ergebnisse und Aktionen (Behebungen, Austausch) werden dokumentiert.

Kritische Schwachstellen werden über den ISMS-Prozess bearbeitet. Kritische Schwachstellen, die dem TSP mitgeteilt wurden, werden innerhalb von 48 Stunden vom ISMS-Team bewertet und ein Lösungsszenario aufgezeigt. Im Falle, dass eine umgehende und vollständige Beseitigung der Schwachstelle nicht möglich ist, wird ein Behandlungsplan erstellt, der die Minderung der kritischen Schwachstellen zum Inhalt hat.

5.5 Datenarchivierung

5.5.1 Art der archivierten Datensätze

Es werden folgende Daten archiviert:

- Alle Registrierungsinformationen, einschließlich
  - der vom Antragsteller im Rahmen der Beantragung einer Ausstellung, Sperrung oder Verlängerung vorgelegte Dokumente und Kontaktangaben,
  - der Identifikationsdaten von Identifikationsdokumenten,
  - falls vorhanden die Methode zur Validierung von Ausweisdokumenten,
  - falls zutreffend der POSTIDENT Unterlagen,
  - der Identität des RA-Mitarbeiters, der den Antrag geprüft, freigegeben oder abgelehnt hat.
- Alle wesentlichen Ereignisse zum Lebenszyklus der Zertifikate (Beantragung, Prüfung, Freigabe, Ablehnung, Ausstellung, Sperrung, Erneuerung.)
- Alle veröffentlichten CPS.
- Zertifizierungsunterlagen und Auditberichte.
- Ggf. weitere Informationen, die zur Gewährleistung der Kontinuität der Dienste erforderlich sind.
- Ggf. weitere Informationen, die ausgegeben und empfangen wurden, und als Beweismittel in Gerichtsverfahren benötigt werden könnten.
- Alle Audit-/Event-Logging-Dateien, die gemäß Kapitel 5.4 erfasst werden.

Unter Berücksichtigung der relevanten Datenschutzaspekte werden weitere Daten archiviert (z.B. E-Mails, elektronische zugesendete Dokumente).

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Folgende Aufzeichnungen und Aufbewahrungszeiträume werden festgelegt:

- Auftragsunterlagen, insbesondere Informationen zu Zertifikatsanträgen, deren Validierung, sowie die daraus resultierenden Zertifikate und vorgenommener Sperrungen, werden 10 Jahre nach Ablauf der Zertifikatsgültigkeit vorgehalten,
- bei ServerPass EV bis zur Betriebsbeendigung, aber mindestens 10 Jahre nach Ablauf der Zertifikatsgültigkeit,
- Audit- und Event Logging Daten werden entsprechend den aktuellen gesetzlichen Bestimmungen archiviert.

5.5.3 Schutz von Archiven

Das Trust Center stellt sicher, dass nur autorisierte und vertrauenswürdige Personen Zutritt zu Datenträgerarchiven erhalten. Archivdaten sind gegen unbefugte Lesezugriffe, Änderungen, Löschungen oder andere Manipulationen geschützt.

5.5.4 Sicherungsverfahren für Archive

Eine inkrementelle Sicherung der elektronischen Archive wird täglich durchgeführt.

5.5.5 Anforderungen an Zeitstempel von Datensätzen

Datensätze wie beispielsweise Zertifikate, Zertifikatssperrlisten, OSCP-Antworten, Logging-Dateien enthalten Informationen über Datum und Uhrzeit. Als Zeitquelle dient eine NTP-Appliance (mit GPS- und DCF77-Antenne), aus der die UTC Zeit abgeleitet wird. Die einzelnen Systeme gleichen die Systemzeit mit der Zeitquelle mehrmals am Tag ab.

5.5.6 Archiverfassungssystem (intern oder extern)

Das Trust Center verwendet ausschließlich interne Archivierungssysteme.

5.5.7 Verfahren zur Beschaffung und Überprüfung von Archivinformationen

Nur autorisiertes und vertrauenswürdiges Personal erhält Zutritt zu Archiven und Zugang/ Zugriff zu Archivdaten. Bei der Wiederherstellung der Archivdaten werden diese auf Authentizität verifiziert.

5.6 Schlüsselwechsel

Innerhalb des Gültigkeitszeitraums kann ein Schlüsselwechsel bzw. Zertifikatswechsel in folgenden Fällen erforderlich werden

- Kompromittierung des Schlüsselmaterials,
- zwingende Änderung des Kryptoalgorithmus,
- zwingende Änderung der Schlüssellänge,
- Änderung des Zertifikatsinhalts.

Die Generierung neuer Schlüssel und Zertifikate wird dokumentiert und gemäß den Regelungen des Schlüsselgenerierungsverfahrens (Key Generation Ceremony) überwacht. Neue Zertifikate und ihre Fingerprints werden veröffentlicht (siehe hierzu Kapitel 2.3). Zertifikate können nur innerhalb des Gültigkeitszeitraums der hierarchisch übergeordneten Root-CA erneuert werden. Abgelaufene oder gesperrte Zertifikate stehen weiterhin zu Validierung auf einer Webseite zur Verfügung.

5.7 Kompromittierung und Notfall-Wiederherstellung

5.7.1 Verfahren zur Meldung und Behandlung von Vorfällen und Kompromittierungen

Die Notfalldokumentation des Trust Centers berücksichtigt die Anforderungen der Telekom Security CP.

Die Mitarbeiter des Trust Centers verfügen über mehrere Möglichkeiten (technische Schnittstelle, direkter Kontakt zum ISMS, Mitarbeiter-Portal) zur Meldung von (Informationssicherheits-)Vorfällen und sind dazu verpflichtet, Vorfälle zu melden. Meldungen bzw. Alarmen wird durch qualifiziertes Personal entsprechend der Kritikalität in angemessener Zeit nachgegangen.

5.7.2 Beschädigung von EDV-Geräten, Software und/oder Daten

Bei einer Beschädigung der EDV-Komponenten, Software und/oder Daten wird der Vorfall unmittelbar untersucht und der Trust Center Sicherheitsabteilung (dem Informationssicherheitsbeauftragten) gemeldet. Das Ereignis initiiert eine entsprechende Eskalation, Störfalluntersuchung, Störfallreaktion bis hin zur finalen Störungsbeseitigung. Abhängig von der Störungsklassifizierung erfolgt die Wiederherstellung (Disaster Recovery). Jegliche Hard- und Software, die zur Bereitstellung des Services TeleSec ServerPass erforderlich ist, wird als Vermögensgegenstand (Asset) und Anwendung im Konfigurationsmanagement der DT Security GmbH geführt.

5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln von Zertifizierungsstellen

Bei Kenntnisnahme einer Kompromittierung des privaten Schlüssels einer CA wird der Vorfall unmittelbar untersucht, beurteilt und die notwendigen Schritte eingeleitet.

Endteilnehmer werden über die mögliche Kompromittierung über die einschlägigen Webseiten informiert (siehe hierzu Kapitel 2.3). Falls erforderlich ist/sind das/die Zertifikate unverzüglich zu sperren und die entsprechende Zertifizierungsstellen-Sperrliste (ARL) zu generieren und zu veröffentlichen.

5.7.4 Geschäftskontinuität nach einem Notfall

Das Trust Center hat für den Rechenzentrumsbetrieb einen Notfallplan entwickelt, implementiert und getestet, um die Auswirkungen von Katastrophen jeder Art (Naturkatastrophen oder Katastrophen menschlichen Ursprungs) zu mildern und die Verfügbarkeit kritischer Geschäftsprozesse schnellstmöglich wiederherzustellen. Dies umfasst auch alle Prozesse, Komponenten, Systeme und Dienste des Trust Centers. Dieser Plan wird mindestens jährlich überprüft, getestet und entsprechend aktualisiert, um im Falle einer Katastrophe gezielt und strukturiert reagieren zu können.

Der Notfallplan enthält mindestens die folgenden Informationen:

- Die notwendigen Kriterien für die Aktivierung des Planes
- Mögliche Notfallmaßnahmen (je nach Situation)
- Ausweichverfahren
- Wiederanlauf Verfahren
- Prozedur zur regelmäßigen Pflege, Aktualisierung und Weiterentwicklung

- Sensibilisierungsmaßnahmen
- Anforderungen an Aus- und Weiterbildung des betroffenen Personals
- Die Verantwortung der Individuen (Rollenbeschreibung und -zuweisung)
- Wiederanlaufzeit (RTO)
- Regelmäßige Durchführung der Notfallpläne zu Testzwecken
- Eine Prozedur zur Aufrechterhaltung oder fristgerechten Wiederherstellung der ServerPass Geschäftstätigkeit nach Unterbrechung oder Ausfall kritischer Geschäftsprozesse
- Eine Verpflichtung kritische kryptographische Geräte und Informationen an einem anderen Standort zu sichern bzw. vorzuhalten.
- Festlegung der maximal tolerierbaren Ausfallzeit (MTD) und entsprechende Zeiten zur Wiederherstellung
- Häufigkeit, in der von kritischen Geschäftsinformationen und eingesetzter Software inkl. deren Konfiguration Sicherungskopien erstellt werden
- Räumliche Entfernung des oder der Ausweichstandorte bzw. -Einrichtungen zur ServerPass Hauptgeschäftsstelle bzw. zum Rechenzentrum des Trust Centers
- Verfahren zur bestmöglichen Sicherung der Betriebsstätten und –Einrichtungen nach einer Katastrophe (Notbetrieb) bis zur Wiederherstellung eines den Anforderungen entsprechend gesicherten Normalbetriebs.

Im Rahmen eines Compliance-Audits (siehe Kapitel 8) ist der Auditor berechtigt, die Details des Notfallplanes einzusehen.

5.8 Betriebsbeendigung einer Zertifizierungs- oder Registrierungsstelle

5.8.1 Beendigung der Zertifizierungsstelle

Die Betriebsbeendigung der Zertifizierungsstelle oder der Registrierungsstelle kann nur durch die DT Security GmbH ausgesprochen werden.

Es werden wirtschaftlich angemessene (oder einzelvertraglich zugesagte) Anstrengungen unternommen, um betroffene untergeordnete Stellen (Endteilnehmer, Registrierungsstellen) vorab über diese Betriebsbeendigungen zu informieren.

Im Falle der Einstellung des Zertifizierungsdienstes geht die Zertifizierungsstelle entsprechend den Vorgaben aus [ETSI EN TSP] Kap. 7.12 vor und hat dafür einen Beendigungsplan erstellt, der folgende Maßnahmen beschreibt:

- Benachrichtigung der Endteilnehmer und Vertrauende Dritte über die geplante Einstellung des Dienstes,
- Fortführung der Sperrfunktionalitäten einschließlich der regelmäßigen Erstellung von Sperrlisten, Abruf der Zertifikatsstatusinformationen und Service Desk-Funktionen,
- Sperrung der involvierten Sub-CA-Zertifikaten,
- eventuell erforderliche Übergangsregelungen auf eine Nachfolge-CA,
- je nach Ausgestaltung bestehender Einzelverträge entstehende Kostenerstattung,
- Aufbewahrung der Unterlagen und Archive der Zertifizierungsstelle (CA)

Vor der Einstellung des Dienstes werden alle möglichen Maßnahmen getroffen, um den potentiellen Schaden für alle Beteiligten möglichst gering zu halten, alle Beteiligten werden so früh wie möglich informiert.

Alle Rechte der Mitarbeiter der Zertifizierungsstelle und der Registrierungsstellen werden entzogen, die privaten Schlüssel der CA werden vernichtet. Alle noch gültigen Zertifikate werden gesperrt.

Alle elektronisch erfassten Daten mit Ausnahme der Zertifikate und Sperrlisten werden gelöscht. Die Zertifikate und Sperrlisten sowie Papierdokumente werden archiviert, um ggf. zur Beweissicherung in Gerichtsprozessen darauf zugreifen zu können.

6 TECHNISCHE SICHERHEITSKONTROLLEN

Die technischen Sicherheitsmaßnahmen sind in einem Sicherheitskonzept festgelegt, deren Wirksamkeit ist auf Basis einer Bedrohungsanalyse nachgewiesen. Es werden die Vorgaben aus [ETSI EN TSP] Kap. 7.5 umgesetzt.

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren

Alle Schlüssel genügen den in Kap. 6.1.5 und 6.1.6 aufgeführten Algorithmen, Schlüssellängen und Qualitätsanforderungen. Die technischen und organisatorischen Vorgaben zur Generierung der verschiedenen Schlüssel werden nachfolgend aufgeführt.

6.1.1.1 Generierung von Root-CA-Schlüsselpaaren

Nicht anwendbar.

6.1.1.2 Generierung von Sub-CA-Schlüsselpaaren

Sub-CA-Schlüsselpaare werden in einem Kryptomodul gemäß Kap. 6.2.1 in der sicheren Umgebung der Sub-CA, die diese Schlüssel nutzen möchte, generiert.

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

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

Die Generierung erfolgt durch mindestens zwei vertrauenswürdige Mitarbeiter des TSP. Jeder der beiden Mitarbeiter hat Kenntnis von einem Teil der zur Schlüsselgenerierung erforderlichen Aktivierungsdaten aber keine Kenntnis über die kompletten Aktivierungsdaten.

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

6.1.1.3 Generierung von RA-Schlüsselpaaren

Die TSP generieren RA Schlüsselpaare in kryptografischen Modulen gemäß Kap. 6.2.1.

6.1.1.4 Generierung von Endteilnehmer-Schlüsselpaaren

Nicht anwendbar.

Eine Generierung von Schlüsselpaaren für Endteilnehmer findet nicht statt. Der Endteilnehmer generiert das Schlüsselpaar eigenverantwortlich mit Tools, die von der Serverapplikation zur Verfügung gestellt werden.

6.1.2 Zustellung privater Schlüssel an Endteilnehmer

Der private Schlüssel des Endteilnehmers verbleibt immer beim Endteilnehmer. Eine Zustellung privater Schlüssel an Endteilnehmer findet nicht statt. Es werden keine privaten Schlüssel im Auftrag des Kunden generiert.

6.1.3 Zustellung öffentlicher Schlüssel an Zertifikatsaussteller (CA)

Alle Endteilnehmer reichen, nach erfolgreicher Authentifikation, den zu zertifizierenden öffentlichen Schlüssel in elektronischer Form (PKCS#10-Request) über eine durch TLS/SSL gesicherten Verbindung bei der Zertifizierungsstelle ein.

6.1.4 Zustellung öffentlicher CA-Schlüssel an vertrauende Dritte

Das Root-CA-Zertifikat, das für die Bildung der Vertrauenskette (Zertifikatsvalidierung) erforderlich sind, wird für alle Endteilnehmer und Vertrauende Dritte durch die Einbettung in die Zertifikatsspeicher der Betriebssysteme und Applikationen (z.B. Web-Browsern) zur Verfügung gestellt. Darüber hinaus werden die Zertifikate für Endteilnehmer mit allen CA-Zertifikaten (außer Root-CA) der Vertrauenskette ausgeliefert. Auf den Internetseiten des TSP stehen die erforderlichen Root-CA- und CA-Zertifikate ebenfalls zur Verfügung.

6.1.5 Schlüssellängen

Um nicht mit Hilfe der Kryptoanalyse private Schlüssel ermitteln zu können, müssen die Schlüssellängen innerhalb des definierten Verwendungszeitraums über eine ausreichende Länge verfügen.

Für Sub-CA- und Endteilnehmer-Zertifikate werden die Anforderungen bzgl. Schlüssellängen und Algorithmen der Baseline Requirements [CABF-BR] und [SOGIS] erfüllt.

6.1.6 Generierung und Qualitätsprüfung öffentlicher Schlüsselparameter

Der während der Beauftragung eingereichte Zertifikatsrequest (PKCS#10) wird auf die folgenden Qualitätsparameter geprüft:

- Der öffentliche Schlüssel ist kein Debian Weak Key.
- RSA: Die durch 8 teilbare Schlüssellänge beträgt 2048 Bit, 3072 Bit oder 4096 Bit.
- RSA: Der Wert des Exponenten ist eine ungerade Zahl größer oder gleich 3 und liegt im Bereich von 2^{16} und 2^{256}-1.
- RSA: Der Wert des Modulus ist eine ungerade Zahl, die nicht die Potenz einer Primzahl ist und keine Faktoren hat, die kleiner als 752 sind.
- ECC: Der öffentliche Schlüssel stammt aus einer der folgenden Kurven:
    - prime256v1 [NIST P-256, Windows-Anzeige ECDH_P256]
    - secp384r1 [NIST P-384, Windows-Anzeige ECDH_P384]
- ECC: Der öffentliche Schlüssel kann erfolgreich mit der ECC-Routine zur vollständigen Validierung geprüft werden.
- Alle Linter-Prüfungen konnten erfolgreich durchgeführt werden.
- Der öffentliche Schlüssel ist für die Zertifizierungsstelle einmalig.
- Als Signatur-Hash-Algorithmus wird mindestens SHA-256 im Zertifikatsrequest verwendet. (SHA-1 wird aktuell noch zugelassen. Es wird aber ein Warnhinweis angezeigt, dass der Wechsel auf SHA-256 oder höher empfohlen wird.)

Wenn eine der Prüfungen fehlschlägt, wird der Zertifikatsauftrag abgelehnt. Die Einhaltung der Qualitätsparameter für CA-Schlüssel des TSPs werden durch die in Kap. 6.2 beschriebenen technischen Kontrollen der verwendeten kryptografischen Module sichergestellt.

6.1.7 Schlüsselverwendungen (gemäß X.509v3-Erweiterung „key usage“)

Siehe Kapitel 7.1.2.5.

6.2 Schutz privater Schlüssel und technische Kontrollen kryptografischer Module

Das Trust Center hat physikalische, organisatorische und prozessuale Mechanismen implementiert, um die Sicherheit von CA- Schlüsseln gewährleisten zu können.

Endteilnehmer sind verpflichtet, alle erforderlichen Vorkehrungen zu treffen, um den Verlust, die Offenlegung oder die unberechtigte Nutzung von privaten Schlüsseln zu verhindern.

6.2.1 Standards und Kontrollen für kryptografische Module

Die privaten Schlüssel der CAs werden auf einem FIPS 140-2/ Level 3 evaluiertem Hardware Security Modul (HSM) abgelegt. Die Sicherung der Schlüssel wird unter Verwendung hochwertiger Mehrpersonen-Sicherungstechniken (siehe auch Kapitel 6.2.2) durchgeführt.

Zum Schutz der kryptographischen Geräte während Betrieb, Transport und Lagerung werden die Hersteller-spezifischen Mechanismen verwendet, die während der FIPS- und CC-Zertifizierungen geprüft wurden. Die Geräte werden hierbei getrennt von den zum Betrieb und zur Nutzung benötigten PED-Keys aufbewahrt, so dass die Kompromittierung einer einzelnen Lokation nicht ausreicht, um die Geräte missbräuchlich zu verwenden.

Vor In- und Außerbetriebnahme werden Integritäts- und Funktionstest dokumentiert durchgeführt.

6.2.2 Mehrpersonenkontrolle (m von n) bei privaten Schlüsseln

Das Trust Center hat technische, organisatorische und prozessuale Mechanismen implementiert, die die Teilnahme mehrerer vertrauenswürdiger und geschulter Personen des Trust Centers (Trusted Roles) erfordern, um vertrauliche kryptografische CA-Operationen durchführen zu können. Die Verwendung des privaten Schlüssels wird durch einen geteilten Authentisierungsprozess (Trusted Path Authentification mit Key) geschützt. Jede am Prozess beteiligte Person verfügt über Geheimnisse, die nur in der Gesamtheit bestimmte Arbeiten ermöglichen.

6.2.3 Hinterlegung von privaten Schlüsseln

Eine Hinterlegung von privaten Schlüsseln bei Treuhändern außerhalb des Trust Centers wird nicht durchgeführt.

6.2.4 Sicherung von privaten Schlüsseln

Das Trust Center behält für Wiederherstellungs- und Notfallzwecke Sicherungskopien (Back-Up) des Schlüsselmaterials jedes CA-Zertifikates vor. Diese Schlüssel werden in verschlüsselter Form innerhalb des kryptografischen Hardware-Moduls (HSM) und zugehörigen Schlüsselspeichergeräten gespeichert.

Weiterhin gibt es Sicherungen der privaten CA-Schlüssel der ServerPass Sub-CAs in gesicherter Umgebung. Der Zugriff auf diese Schlüssel ist nur vertrauenswürdigen Personen des Trust Centers (Trusted Role) gestattet.

Der jeweilige private Schlüssel wird dabei in verschlüsselter Form auf speziellen Security-Tokens gespeichert.

Zur Wiederherstellung eines privaten Schlüssels einer CA, d.h. einspielen des Schlüssels in die CA-Software, werden ebenfalls mehrere vertrauenswürdige Personen des Trust Centers

(Trusted Role) benötigt. Eine Wiederherstellung darf nur innerhalb der Hoch-Sicherheitszone des Trust Centers erfolgen.

Das Trust Center bietet für ServerPass keine Sicherung des privaten Schlüssels im Auftrag des Endteilnehmers an.

6.2.5 Archivierung von privaten Schlüsseln

Wenn Sub-CA- oder OCSP-Schlüssel das Ende ihrer Gültigkeitsdauer erreicht haben, werden sie vernichtet. Eine Archivierung findet nicht statt.

Das Trust Center bietet keine Archivierung des privaten Schlüssels im Auftrag des Endteilnehmers an.

6.2.6 Übertragung privater Schlüssel in oder von einem kryptografischen Modul

Sub-CA-Schlüssel werden auf den kryptografischen Hardware-Modulen (HSM) im Online-Betrieb generiert.

Das Schlüsselmaterial für ein Zertifikat einer Zwischenzertifizierungsstelle (Sub-CA) wird auf einem kryptografischen Hardware-Security-Modul (HSM) im Online-Betrieb generiert. Der zu zertifizierenden öffentliche Schlüssel mit den Daten des Subject-DN wird in elektronischer Form (PKCS#10-Request) auf sicherem Wege auf die Offline-CA übertragen, die das Sub-CA-Zertifikat generiert. Anschließend wird das Sub-CA-Zertifikat auf sicherem Wege auf das HSM der Online-CA übertragen und dem privaten Schlüssel zugeordnet.

6.2.7 Speicherung privater Schlüssel auf kryptografischen Modulen

Das Trust Center speichert CA-Schlüssel in sicherer Form auf kryptografischen Hardware-Security-Modulen (HSM), welche nach FIPS 140-2/ Level 3 evaluiert sind.

6.2.8 Methode zur Aktivierung privater Schlüssel

Alle Endteilnehmer, Registratoren, Administratoren und Operatoren müssen die Aktivierungsdaten (z.B. PIN, Importpasswort) für ihren privaten Schlüssel gegen Verlust, Diebstahl, Änderung, Offenlegung und unbefugte Nutzung gemäß des vorliegenden CPS schützen.

Der zum Sub-CA-Zertifikat gehörende private Schlüssel bleibt aktiv bis das Zertifikat die Gültigkeit verliert oder ein Sperrgrund vorliegt.

6.2.8.1 Private Schlüssel von Endteilnehmern

Der Endteilnehmer verpflichtet sich wirtschaftlich angemessene Maßnahmen zum physikalischen Schutz der verwendeten Hardware/Software zu ergreifen, um die Nutzung des Platzes/Komponente und seines zugehörigen privaten Schlüssels ohne Genehmigung des Endteilnehmers zu verhindern.

6.2.8.2 Private Schlüssel von Administratoren

Der Administrator oder Operator hat zum Schutz des privaten Schlüssels folgende Vorgaben einzuhalten:

- Festlegung eines Passworts bzw. einer PIN (gemäß Kapitel 6.4.1) oder Integration einer gleichwertigen Sicherheitsmaßnahme, um den Administrator oder Operator vor der Aktivierung des privaten Schlüssels zu authentisieren. Dies kann z. B. auch ein Kennwort

zum Betrieb des privaten Schlüssels, ein Windows Anmelde- oder Bildschirmschonerkennwort, ein Anmeldekennwort für das Netzwerk beinhalten.
- Ergreifung geeigneter Maßnahmen zum physischen Schutz des Administrator- oder Operator-Arbeitsplatzes vor unberechtigtem Zugriff.

6.2.8.3 Private Schlüssel von Sub-CA und Root-CA-Zertifikaten

Schlüsselmaterial für CA- und Root-CA-Zertifikate wird entsprechend durch die autorisierten Personen aktiviert und auf kryptographischen Hardware-Modulen (HSM) aufgebracht (Kapitel 6.2.2 und 6.4.1).

Der zum CA-Zertifikat gehörende private Schlüssel bleibt aktiv bis das Zertifikat die Gültigkeit verliert oder ein Sperrgrund vorliegt.

Der zum Root-CA-Zertifikat gehörende private Schlüssel wird nur zur Erzeugung von weiteren CA-Zertifikaten aktiviert. Nach Ablauf des Root-CA-Zertifikats wird der private Schlüssel nicht mehr genutzt.

6.2.9 Methode zur Deaktivierung privater Schlüssel

Die Deaktivierung privater Schlüssel von Administratoren und Operatoren erfolgt ereignisbezogen und obliegt dem Personal des Trust Centers.

Für die Deaktivierung von privaten Endteilnehmer Schlüsseln ist der Endteilnehmer verantwortlich.

Private Schlüssel, welche zu ServerPass CA-Zertifikaten gehören, werden prinzipiell vernichtet (siehe 6.2.10) und in keinem Fall deaktiviert.

6.2.10 Methode zur Vernichtung privater Schlüssel

Die Vernichtung von CA-Schlüsseln erfordert die Teilnahme mehrerer vertrauenswürdiger Personen (Trusted Roles) des Trust Centers. Dabei ist sicherzustellen, dass nach Vernichtung keine Fragmente des Schlüssels übrigbleiben, die zu einer Rekonstruktion des Schlüssels führen könnte. Das Trust Center verwendet zur sicheren Schlüsselvernichtung eine integrierte Löschfunktion des HSM.

Die Vernichtung privater Schlüssel des Endteilnehmers obliegt diesem selbst.

6.2.11 Bewertung kryptografischer Module

Siehe Kapitel 6.2.1.

6.3 Andere Aspekte der Verwaltung von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Das Trust Center sichert und archiviert im Rahmen regelmäßiger Sicherungsmaßnahmen die Zertifikate (CA-, Root-CA und Endteilnehmer-Zertifikate).

6.3.2 Gültigkeitsdauer von Zertifikaten und Schlüsselpaaren

Die Zertifikatsgültigkeit beginnt mit der Generierung des Zertifikats. Mit dem Ablauf des Gültigkeitszeitraums oder durch Sperrung endet die Zertifikatsgültigkeit. Die Gültigkeitsdauer von Schlüsselpaaren entspricht der Gültigkeitsdauer des zugehörigen Zertifikats.

In **Fehler! Verweisquelle konnte nicht gefunden werden.** sind die Gültigkeitszeiträume der CA-Zertifikate dargestellt.

Das Trust Center stellt sicher, dass die CA-Zertifikate vor Ablauf ausgewechselt werden, um die entsprechende Zertifikatsgültigkeit von Endteilnehmer-Zertifikaten gewährleisten zu können.

Tabelle 3: Gültigkeit von Zertifikaten

Zertifikatstyp:	**Gültigkeitsdauer:**
TeleSec ServerPass Standard und SAN/UCC	
TeleSec ServerPass Class 2 CA	10 Jahre
T-TeleSec GlobalRoot Class 2	25 Jahre
Endteilnehmer-Zertifikate	1 Jahr. Der Kulanzzeitraum beträgt 5 Tage.
TeleSec ServerPass EV/EV SAN, QWAC	
TeleSec ServerPass Extended Validation Class 3 CA	10 Jahre
T-TeleSec GlobalRoot Class 3	25 Jahre
Endteilnehmer-Zertifikate	1 Jahr. Der Kulanzzeitraum beträgt 5 Tage.
Sonstige Zertifikate	
OCSP-Signer <Root-CA>	3 Monate
OCSP-Signer <Sub-CA>	1 Monat

6.4 Aktivierungsdaten

6.4.1 Generierung und Installation von Aktivierungsdaten

Um die auf dem HSM hinterlegten privaten Schlüssel der CA-Zertifikate schützen zu können, werden Aktivierungsdaten (Geheimnisanteile) nach den in Kapitel 6.2.2 dieser CPS beschriebenen Anforderungen und dem Dokument „Key Ceremony“ generiert. Die Erstellung und Verteilung von Geheimnisanteilen wird protokolliert.

6.4.2 Schutz von Aktivierungsdaten

Die Trust Center Administratoren bzw. vom Trust Center autorisierten Personen verpflichten sich, die Geheimnisanteile für die Aktivierung der privaten Schlüssel der Root-CA-, CA- und OCSP-Zertifikate zu schützen.

6.4.3 Weitere Aspekte von Aktivierungsdaten

6.4.3.1 Übertragung von Aktivierungsdaten

Sofern Aktivierungsdaten für private Schlüssel, unabhängig vom Übertragungsmedium, übertragen werden, müssen die Trust Center-Administratoren die Übertragung mithilfe von Methoden zum Schutz gegen Verlust, Diebstahl, Änderung, unbefugter Offenlegung oder Nutzung dieser privaten Schlüssel strengstens schützen.

6.4.3.2 Vernichtung von Aktivierungsdaten

Nach dem Löschen der privaten Schlüssel (Kapitel 6.2.4) sind die Aktivierungsdaten nicht mehr schützenswert.

6.5 Computer-Sicherheitskontrollen

Das Trust Center führt alle PKI-Funktionen mit Hilfe vertrauenswürdiger und geeigneter Systeme durch.

Die Systeme werden von Monitoring-Systemen fortlaufend auf Funktion und Kapazität geprüft, so dass im Bedarfsfall zeitnah eine Erweiterung von Ressourcen durchgeführt werden kann. Die Sicherheitsmaßnahmen für Computer der Zertifizierungsstelle (z.B. Netzwerksicherheit, Zugriffskontrolle, Überwachung etc.) sind im Sicherheitskonzept beschrieben. Es werden die Vorgaben aus [ETSI EN 319 401] Kap. 7.4 umgesetzt.

Die Systeme für Entwicklung, Test (TU) und Produktion (PU) sind vollkommen getrennt voneinander aufgebaut, sie befinden sich auf unterschiedlicher Hardware in verschiedenen Netzsegmenten, so dass eine gegenseitige Beeinflussung ausgeschlossen ist.

6.5.1 Spezifische technische Anforderungen an die Computersicherheit

Das Trust Center setzt ausschließlich vertrauenswürdige Systeme ein, welche die technische Sicherheit und Zuverlässigkeit der von den Systemen unterstützten Prozesse gewährleisten. Alle Systeme für das Zertifikatsmanagement sowie die Status- und Verzeichnisdienste werden im Risikomanagement des Trust Centers berücksichtigt und entsprechend ihrer Kritikalität bzw. dem Schadenspotenzial geschützt.

Die geforderte Trennung von vertrauenswürdigen Rollen (siehe Kap. 5.2.4) wird von allen notwendigen Systemen technisch unterstützt. Insbesondere werden die Accounts der für den Betrieb der kritischen Systeme erforderlichen vertrauenswürdigen Rollen (siehe Kap. 5.2.1) so verwaltet, 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. Alle Accounts werden regelmäßig, mindestens aber alle 3 Monate, geprüft und bei Bedarf in angemessener Zeit geändert oder gelöscht.

Die Administrationssysteme zur Umsetzung der Sicherheitsrichtlinien werden ausschließlich für diesen und keine anderen Zwecke verwendet.

Die CA-, Zertifikatsmanagement-, Sicherheits- und Frontend-Systeme sowie, falls anwendbar, weitere interne Systeme zur Unterstützung des Betriebs werden standardmäßig nach konzernweiten Vorgaben bzw. Best Practices gehärtet, d.h. für den Betrieb der CAs nicht benötigte Accounts, Dienste, Protokolle und Ports werden deaktiviert.

Die Systeme der Telekom Security werden mit einem Integritätsschutz versehen, der vor Viren, Schadcode und dem Einspielen unerlaubter Software schützt, und hinsichtlich Auslastung und verfügbarer Ressourcen überwacht, um einen ununterbrochenen Betrieb zu gewährleisten. Diese und weitere Sicherheitsmaßnahmen für Systeme des Trust Centers sind im Sicherheitskonzept beschrieben.

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

Die Entwicklungs-, Test- und Produktivumgebungen des Trust Centers werden auf unterschiedlicher Hardware in unterschiedlichen Netzsegmenten betrieben und sind daher gänzlich voneinander getrennt.

6.5.2 Bewertung der Computersicherheit

Nach jeder signifikanten System- oder Netzwerkänderung erfolgt innerhalb einer Woche, mindestens jedoch einmal je Kalenderquartal eine automatisierte Schwachstellenüberprüfung (Vulnerability-Scan). Mögliche Schwachstellen werden analysiert, bewertet und registriert. Basierend auf der Auswertung werden Maßnahmen festgelegt und in einem definierten Plan umgesetzt. Die Schwachstellenüberprüfungen, ihre Ergebnisse und Aktionen (Behebungen, Austausch) werden dokumentiert.

Kritische Schwachstellen werden über den ISMS-Prozess bearbeitet. Kritische Schwachstellen werden innerhalb von 48 Stunden vom ISMS-Team bewertet und ein Lösungsszenario aufgezeigt. Wenn eine umgehende und vollständige Beseitigung der Schwachstelle nicht möglich ist, wird ein Behandlungsplan erstellt, der die Minderung der kritischen Schwachstellen zum Inhalt hat.

Zusätzlich werden einmal jährlich sogenannte Penetrationstests durchgeführt. Auch hier werden entsprechend Maßnahmen abgeleitet und umgesetzt, sofern dies notwendig ist. Die Penetrationstest und Schwachstellenscans werden von dafür geschultem Personal durchgeführt. Die eingesetzten Werkzeuge entsprechen dabei dem aktuellen Stand der Technik.

6.6 Technische Kontrollen des Lebenszyklus

6.6.1 Systementwicklungskontrollen

Das Trust Center hat Mechanismen und Kontrollen implementiert, um eingekaufte, entwickelte oder veränderte Software auf Schadelemente oder bösartigen Code (z.B. Trojaner, Viren) überwachen und schützen zu können. Die Integrität wird vor der Installation manuell verifiziert.

Neue Software-Versionen der Software (geplante Updates) oder Fehlerbeseitigungen (kurzfristige Bugfixes) werden zunächst auf einem Entwicklungssystem des Herstellers/Entwicklers bereitgestellt und getestet.

Nach Prüfung erfolgt die Installation auf einem Testsystem. Erst nach ausgiebigen und erfolgreichen Tests erfolgt die Installation auf dem Wirksystem.

Die Verwaltung der PKI-Systeme (CA, HSM, Web-Server, …) durch die Systemadministratoren erfolgt über ein getrenntes Netz das ausschließlich diesen Rolleninhabern zur Verfügung steht. Die Verwaltung anderer IT-Systeme (nicht PKI-Systeme) über dieses Netz ist unzulässig.

Das bei der DT Security GmbH etablierte Change-Management findet Anwendung.

6.6.2 Maßnahmen des Sicherheitsmanagements

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

Alle Änderungen, die sich auf das festgelegte Sicherheitsniveau auswirken, werden zuvor von der Leitung des Trust Centers freigegeben.

Das Schwachstellenmanagement des Trust Centers ist so geregelt, 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.

Die Systeme loggen, soweit möglich, alle sicherheitsrelevanten Ereignisse. Dabei werden die Systeme unter anderem auf folgende Aktivitäten überwacht (inkl. geeigneter Alarmierungsfunktionen):

- Sicherheitsrelevante Systemereignisse, dazu zählen:
    - erfolgreiche und erfolglose Zugriffsversuche auf die Zertifikatssysteme,
    - durchgeführte Tätigkeiten an den Zertifikats- und Sicherheitssystemen,
    - Starten und Abschalten der Protokollierungsfunktionen,
- Verfügbarkeit und Nutzung der benötigten Dienste,
- Änderungen von Sicherheitsprofilen,
- Installation, Aktualisierung und Entfernung von Software auf einem Zertifikatssystem,
- Systemabstürze, Hardware-Ausfälle und andere Anomalien,
- Firewall und Router-Aktivitäten und
- Zu- und Austritte in und aus den Betriebsräumen der Zertifikatsmanagementsysteme.

Die Integrität der Systeme inklusive ihrer relevanten (Konfigurations-)Einstellungen wird kontinuierlich auf Änderungen überwacht. Bei Änderungen, die nicht auf Basis eines autorisierten Change durchgeführt wurden, wird den daraus resultierenden Alarmmeldungen durch qualifiziertes Personal nachgegangen.

Die Telekom Security überwacht den Kapazitätsbedarf der Systeme, um sicherzustellen, dass dauerhaft angemessene Verarbeitungsleistungen und Speicherkapazitäten zur Verfügung stehen.

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

6.6.3 Sicherheitskontrollen des Lebenszyklus

Das Trust Center hat Mechanismen und Kontrollen implementiert, dass Sicherheitspatches innerhalb einer angemessenen Zeit, nachdem sie verfügbar sind, installiert werden. Die Integrität des Sicherheitspatches wird vor der Installation manuell verifiziert.

Ein Sicherheitspatch wird nicht installiert, wenn zusätzliche Sicherheitslücken oder Instabilitäten entstehen, die die Vorteile der Anwendung des Sicherheitspatches überwiegen. Der Grund für die Nichtanwendung von Sicherheitspatches wird dokumentiert

6.7 Netzwerk-Sicherheitskontrollen

Es werden die Vorgaben aus [ETSI EN 319 401] Kap. 7.8 umgesetzt.

Die internen Netze und Systeme werden mithilfe von mehrstufigen Firewalls, IDS und IPS, Zoning sowie weiteren Schutzmaßnahmen vor unautorisierten Zugriffen und Angriffen geschützt. Alle Netzwerkkomponenten sind dabei so konfiguriert, dass nur die minimal erforderlichen Protokolle, Dienste und Zugänge verfügbar sind.

Die Segmentierung des Netzwerks basiert auf einer Risikobetrachtung unter Berücksichtigung der funktionalen, logischen und physischen (einschließlich Standort) Beziehungen zwischen vertrauenswürdigen Systemen und Diensten.

Alle für den CA-Betrieb kritischen Systeme werden in sicheren oder hochsicheren Zonen untergebracht. Die Kommunikation zwischen Systemen innerhalb der Sicherheitszonen wird durch entsprechend implementierte und konfigurierte Sicherheitsverfahren geschützt.

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

Innerhalb einer Zone gelten für alle Systeme die gleichen Mindestsicherheitsanforderungen.

Zwischen den Zonen sind Firewalls implementiert, welche die Systeme und Kommunikation innerhalb der sicheren Zonen sowie die Kommunikation mit den Systemen außerhalb der Zonen schützen. Die Verbindungen sind so eingeschränkt, dass nur die zum Betrieb erforderlichen Verbindungen möglich sind, nicht benötigte Verbindungen werden explizit verboten oder deaktiviert.

Die Konfigurationen der Systeme werden hinsichtlich der Einhaltung dieser Regeln in regelmäßigen Abständen und bei Bedarf geprüft.

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

Die Kommunikation zwischen allen vertrauenswürdigen sowie weiteren Systemen ist grundsätzlich auf mehreren Schichten verschlüsselt und wird für fast alle Systeme, mindestens jedoch für die vertrauenswürdigen Systeme, über vertrauenswürdige Kanäle realisiert, die sich logisch von anderen Kommunikationskanälen unterscheiden und eine sichere Identifizierung ihrer Endpunkte gewährleisten.

Alle externen Netzwerkverbindungen sind redundant aufgebaut.

Nach jeder signifikanten System- oder Netzwerkänderung erfolgt i.d.R. innerhalb einer Woche, mindestens jedoch einmal je Kalenderquartal eine automatisierte Schwachstellenprüfung an vom Trust Center identifizierten öffentlichen und privaten IP-Adressen. Die Schwachstellenprüfungen werden von Personen oder Organisationen durchgeführt, die über die für eine zuverlässige Prüfung und Dokumentation erforderlichen Fähigkeiten, Werkzeuge, Fertigkeiten, ethischen Grundsätze und Unabhängigkeit verfügen. Die Durchführung einer Schwachstellenprüfung mit Angabe der Qualifikation der prüfenden Person oder Organisation wird durch das ISMS kontrolliert und zusammen mit den Ergebnissen dokumentiert.

Bei Inbetriebnahme, signifikanten Änderungen an der Infrastruktur bzw. Anwendungen, mindestens jedoch einmal pro Jahr werden die Systeme Penetrationstests unterzogen. Die Penetrationstests werden von Personen oder Organisationen durchgeführt, die über die für eine zuverlässige Prüfung und Dokumentation erforderlichen Fähigkeiten, Werkzeuge, Fertigkeiten, ethischen Grundsätze und Unabhängigkeit verfügen. Die Durchführung der

Penetrationstests mit Angabe der Qualifikation der prüfenden Person oder Organisation wird durch das ISMS kontrolliert und zusammen mit den Ergebnissen dokumentiert.

Nach Bekanntwerden einer kritischen Schwachstelle wird diese, sofern es keine guten Gründe gibt, diese Schwachstelle nicht zu beseitigen, i.d.R. innerhalb von 4 Tagen behoben. Sollte eine Behebung innerhalb von 4 Tagen nicht möglich sein, so wird ein Plan zur Minderung der Schwachstelle, inkl. einer Priorisierung der Aktivitäten, erstellt und in dem dort festgelegten Zeitraum abgearbeitet. Sollte entschieden werden, eine Schwachstelle nicht zu beheben, so wir die begründete Entscheidung im ISMS dokumentiert.

6.8 Zeitstempel

Zertifikate, Sperrlisten, Online-Statusprüfungen und andere wichtige Informationen enthalten Datums- und Zeitinformationen, die aus einer zuverlässigen Zeitquelle abgeleitet werden (siehe Kapitel 5.5.5).

7 ZERTIFIKATS-, SPERRLISTEN- UND OCSP-PROFILE

7.1 Zertifikatsprofil

Die von der Zertifizierungsstelle ausgestellten Zertifikate entsprechen folgenden Anforderungen:

- [RFC 5280]
- [X.509]
- [CABF-BR]
- [CABF-BREV]
- ETSI Vorgaben [ETSI WEB], [ETSI POL], [ETSI QC]

X.509v3-Zertifikate müssen mindestens die in Tabelle 4aufgeführten Inhalte aufweisen.

Tabelle 4: Zertifikatsattribute nach X.509.v3

Feld:	**Wert oder Wertbeschränkung:**
Version:	Zertifikatsversion
Seriennummer:	Eindeutiger Wert zur Identifikation des Zertifikats
Signaturalgorithmus:	RSA - SHA-256 SHA384 ECDSA SHA-256 ECDSA (abhängig von der ausstellenden Sub-CA)
Aussteller:	entsprechend Kapitel 7.1.4
Gültig ab:	Zeitbasis Koordinierte Weltzeit (UTC). Gemäß RFC 5280 kodiert.
Gültig bis:	Zeitbasis Koordinierte Weltzeit (UTC). Gemäß RFC 5280 kodiert.
Auftragsteller:	Eindeutiger Name (siehe Kapitel 7.1.4)
Öffentlicher Schlüssel:	Gemäß RFC 5280 kodiert
Erweiterungen:	
Schlüsselverwendung:	Kapitel 7.1.2.5
Zertifikatsrichtlinie:	Kapitel 7.1.2.1
Alternativer Antragstellername:	Kapitel 7.1.2.6
Grundlegende Beschränkungen:	Kapitel 7.1.2.3
Erweiterte Schlüsselverwendung:	Kapitel 7.1.2.4
Sperrlistenverteilungspunkt:	Kapitel 7.1.2.2
Schlüsselkennung des Ausstellers:	Kapitel 7.1.2.7
Schlüsselkennung des Antragstellers:	Kapitel 7.1.2.8
Zugriff auf Stelleninformation	Kapitel 7.1.2.9

QC-Statement	Kapitel 7.1.2.10

Die Zertifikats-Seriennummern werden von ServerPass in nicht sequentieller Nummerierung vergeben und enthalten einen 126-Bit--langen Zufallswert (Entropie).

Zusätzliche Erweiterungen und Eigenschaften (insbesondere auch für Extended Validation Zertifikate) werden in den folgenden Kapiteln ausführlicher erklärt.

7.1.1 Versionsnummer(n)

Die ausgestellten X.509-Zertifikate für Endteilnehmer entsprechen der zurzeit aktuellen Version 3. Die zusätzlichen Erweiterungen und Eigenschaften werden in den folgenden Kapiteln ausführlicher erklärt.

Die Root-CA und Sub-CA-Zertifikate sind ebenfalls vom Typ X.509v3.

7.1.2 Zertifikatserweiterungen

Um den Standard X.509v3 sowie die Guidelines für EV/EV SAN-Zertifikate [CABF-BREV] zu erfüllen, ergänzt die Zertifizierungsstelle das Zertifikatsprofil um entsprechende Erweiterungen. Diese sind in den folgenden Abschnitten beschrieben.

7.1.2.1 Erweiterung „Zertifizierungsrichtlinien“ (certificatePolicies)

Die Erweiterung „Zertifizierungsrichtlinie“ besteht aus einer Objekt Kennung (Object Identifier, OID, siehe auch Kapitel 7.1.6) und einem Link, hinter der diese Zertifizierungsrichtlinie abrufbar ist:

certificatePolicies:policyIdentifier = 2.23.140.1.2.2 (OV) oder

certificatePolicies:policyIdentifier = 2.23.140.1.2.1 (DV) oder

certificatePolicies:policyIdentifier = 2.23.140.1.1 (EV)

certificatePolicies:policyIdentifier = 0.4.0.2042.1.4 (EVCP nur EV/EV SAN)

certificatePolicies:policyIdentifier = 0.4.0.194112.1.4 (QCP-w nur EV/EV SAN)

certificatePolicies:policyQualifiers:policyQualifierId = id-qt 1.

certificatePolicies:policyQualifiers:qualifier = URL zu diesem Dokument.

Der Risikowert dieser Erweiterung ist als “unkritisch” gesetzt.

7.1.2.2 Erweiterung „Sperrlistenverteilungspunkt“ (cRLDistributionPoint)

Alle Endteilnehmer-Zertifikate enthalten einen Sperrlistenverteilungspunkt (cRLDistributionPoint), auf die zugehörige Zertifikatssperrliste (CRL). Vertrauende Dritte benötigen diese URL zur Zertifikatsvalidierung. Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

Das CA-Zertifikat verfügt ebenfalls über einen Sperrlistenverteilungspunkt, über dessen URI (HTTP und LDAP) die aktuelle Sperrliste für Zertifizierungsstellen (ARL) auf dem Verzeichnisdienst abrufbar ist. Vertrauende Dritte benötigen diese URI zur Zertifikatsvalidierung. Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.3 Erweiterung „Grundlegende Beschränkungen“ (BasicConstraints)

Die Erweiterung „grundlegende Beschränkungen“ definiert den Zertifikatstyp (Endteilnehmer, CA) und die Beschränkung der Länge des Zertifizierungspfades (pathLenConstraint).

Bei Endteilnehmer-Zertifikaten ist der Benutzertyp „Endeinheit“ gesetzt (cA = false), die Pfadlänge ist nicht gesetzt. Der Risikowert dieser Erweiterung ist als „kritisch“ gesetzt.

Die Sub-CA-Zertifikate enthalten den Benutzertyp „Zertifizierungsstelle“ mit der Pfadlänge „0“. Der Risikowert dieser Erweiterung ist als „kritisch“ gesetzt.

7.1.2.4 Erweiterung „Erweiterte Schlüsselverwendung“ (ExtendedKeyUsage)

Die Endteilnehmer-Zertifikate enthalten die erweiterte Schlüsselverwendung Client-Authentication (id-kp-clientAuth,1.3.6.1.5.5.7.3.2) und TLS Web Server Authentication (id-kp-serverAuth,1.3.6.1.5.5.7.3.1). Der Risikowert ist als „nicht kritisch“ gesetzt.

7.1.2.5 Erweiterung „Schlüsselverwendung“ (keyUsage)

Die Schlüsselverwendung richtet sich nach den Regeln des RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” und ist darin beschrieben.

In Tabelle 5 und Tabelle 6 sind die Schlüsselverwendungen den unterschiedlichen Zertifikatsprofilen tabellarisch zugeordnet.

Tabelle 5: Zuordnung der Erweiterung „Schlüsselverwendung“

		TeleSec ServerPass Standard und SAN/UCC		
		EE-Zertifikate	Sub-CA-Zertifikate	Root-CA-Zertifikate
	Risikowert (Criticality)	critical	critical	critical
Bit	Bezeichnung			
0	digitalSignature	Ja	Nein	Nein
1	nonRepudation	Nein	Nein	Nein
2	keyEncipherment	(Ja) (nur RSA Schlüssel)	Nein	Nein
3	dataEncipherment	Nein	Nein	Nein
4	keyAgreement	(Ja) (nur ECC Schlüssel)	Nein	Nein
5	keyCertSign	Nein	Ja	Ja
6	CRLSign	Nein	Ja	Ja
7	encipherOnly	Nein	Nein	Nein
8	decipherOnly	Nein	Nein	Nein

Tabelle 6: Zuordnung der Erweiterung „Schlüsselverwendung EV/EV SAN“

		TeleSec ServerPass EV/EV SAN		
		EE-Zertifikat	Sub-CA-Zertifikate	Root-CA-Zertifikate
	Risikowert (Criticality)	critical	critical	critical
Bit	Bezeichnung			
0	digitalSignature	Ja	Nein	Nein
1	nonRepudation	Nein	Nein	Nein
2	keyEncipherment	(Ja) (nur RSA Schlüssel)	Nein	Nein
3	dataEncipherment	Nein	Nein	Nein
4	keyAgreement	(Ja) (nur ECC Schlüssel)	Nein	Nein
5	keyCertSign	Nein	Ja	Ja
6	CRLSign	Nein	Ja	Ja
7	encipherOnly	Nein	Nein	Nein
8	decipherOnly	Nein	Nein	Nein

Im Falle, dass die Schlüsselverwendung als „unkritisch“ deklariert ist, besteht eine erweiterte Schlüsselverwendung (Extended Key Usage), die „kritisch“ markiert ist.

7.1.2.6 Erweiterung „alternativer Antragstellername“ (subjectAltName)

Der Common Name des Distinguished Name wird als alternativer Antragstellername (subjectAltName) eingetragen. Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.7 Erweiterung „Ausstellerschlüsselkennung“ (authorityKeyIdentifier AKI)

Die Erweiterung „Ausstellerschlüsselkennung“ im Feld „Schlüsselkennung“ enthält einen festen 160 Bit langen SHA-1 Hashwert, der mit dem Wert der Erweiterung „Schlüsselkennung des Antragstellers des CA-Zertifikats“ (siehe Kapitel 7.1.2.8) mathematisch übereinstimmt. Dieser Wert wird aus dem Hashwert des öffentlichen Schlüssels der ausstellenden Zertifizierungsstelle gebildet.

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.8 Erweiterung „Antragstellerschlüsselkennung“ (subjectKeyIdentifier)

Die Erweiterung „Schlüsselkennung des Antragstellers“ einen 160 Bit langen SHA-1 Hashwert, der individuell aus dem jeweiligen öffentlichen Schlüssel des aktuellen Zertifikats gebildet wird. Der Hashwert der Erweiterung „Schlüsselkennung des Antragstellers“ stimmt mathematisch mit dem Wert der Erweiterung „Stellenschlüsselkennung“ (siehe Kapitel 7.1.2.7) des hierarchisch darunter liegenden Zertifikats überein.

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.9 Erweiterung „Zugriff auf Stelleninformation“ (Authority Information Access)

In Endteilnehmer-Zertifikaten (EE) enthält die Erweiterung „Zugriff auf Stelleninformation“ die Objekt-Kennung (OID) 1.3.6.1.5.5.7.48.1 für den Dienst OCSP als auch die HTTP-Adresse des OCSP-Responders.

Endteilnehmer-Zertifikat ausgestellt von

- TeleSec ServerPass Class 2 CA: http://ocsp.serverpass.telesec.de/ocspr
- TeleSec ServerPass Extended Validation Class 3 CA: http://ocsp.serverpass.telesec.de/ocspr

In Zwischenzertifizierungsstellen (Sub-CA) enthält die Erweiterung „Zugriff auf Stelleninformation“ die Objekt-Kennung (OID) 1.3.6.1.5.5.7.48.1 für den Dienst OCSP als auch HTTP-URL des jeweiligen OCSP-Responders.

CA-Zertifikate

- TeleSec ServerPass Class 2 CA: http://ocsp.telesec.de/ocspr
- TeleSec ServerPass Extended Validation Class 3 CA: http://ocsp.telesec.de/ocspr

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.1.2.10 Erweiterung „Anweisungen für qualifiziertes Zertifikat“ (qcStatements)

Die Erweiterung „Anweisungen für qualifiziertes Zertifikat“ besteht aus den Objekt Kennungen (Object Identifier, OID) gemäß

- 0.4.0.1862.1.1 = qcStatement - QcCompliance [ETSI QC]
- 0.4.0.1862.1.5 = qcStatement - QcPDS [ETSI QC]
- 0.4.0.1862.1.6 = qcStatement - QcType [ETSI QC]
- 0.4.0.1862.1.6.3 = QcType - id-etsi-qct-web [ETSI QC]

7.1.3 Algorithmus Objekt-Identifier (OID)

7.1.3.1 SubjectPublicKeyInfo

7.1.3.1.1 RSA

Das Feld SubjectPublicKeyInfo für einen RSA-Schlüssel enthält den identifier rsaEncryption (OID: 1.2.840.113549.1.1.1).

Die Parameter sind vorhanden und haben den Wert NULL.

Der AlgorithmIdentifier wird wie folgt kodiert: 300d06092a864886f70d0101010500.

7.1.3.1.2 ECDSA

Das Feld SubjectPublicKeyInfo für einen ECDSA-Schlüssel enthält den identifier id-ecPublicKey (OID: 1.2.840.10045.2.1).

Die Parameter verwenden die namedCurve-Kodierung. Die namedCurve für P-256 Schlüssel ist secp256r1 (OID: 1.2.840.10045.3.1.7) und für P-384 Schlüssel secp384r1 (OID: 1.3.132.0.34).

Der AlgorithmIdentifier für secp256r1 wird wie folgt kodiert:

301306072a8648ce3d020106082a8648ce3d030107.

Der AlgorithmIdentifier für secp384r1 wird wie folgt kodiert:

301006072a8648ce3d020106052b81040022.

7.1.3.2 Signature AlgorithmIdentifier

7.1.3.2.1 RSA

Das Feld Signature AlgorithmIdentifier für RSA enthält den identifier sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

Die Parameter sind vorhanden und haben den Wert NULL.

Der AlgorithmIdentifier wird wie folgt kodiert: 300d06092a864886f70d01010b0500.

7.1.3.2.2 ECDSA

Nicht anwendbar.

7.1.4 Namensformen

Testzertifikate werden im Wirksystem nicht ausgestellt. Stattdessen bieten wir Zertifikate mit 30 Tagen Gültigkeit unter einer nicht öffentlichen Test-CA an.

7.1.4.1 Informationen zum Aussteller

Von TeleSec ServerPass verwendete CA-Zertifikate enthalten einen eindeutigen Ausstellernamen (Issuer DN) gemäß den Ausführungen aus Kapitel 3.1.1.

Die ausgestellten Endteilnehmer-Zertifikate enthalten einen eindeutigen Ausstellernamen (Issuer-DN) der jeweiligen Zertifizierungsstelle.

Der Name des Ausstellers in einem Zertifikat („Issuer-DN“) entspricht dem „Subject-DN“ des ausstellenden Zertifikats „Byte-für-Byte“.

7.1.4.2 Subject-Informationen der Endteilnehmer-Zertifikate

Die Inhalte des Subject-DN (Antragsteller) von Endteilnehmer-Zertifikaten setzen sich wahlweise aus den Feldern wie im Kapitel 3.1.1 beschrieben, zusammen. Die Felder enthalten Pflicht- (mandatory) und optionale Angaben.

7.1.4.2.1 Subject Alternative Name Extension

Siehe Kapitel 3.1.1.1 und 3.1.1.2.

7.1.4.2.2 Subject Distinguished Name Fields

Siehe Kapitel 3.1.1.1 und 3.1.1.2.

7.1.4.3 Subject-Informationen der CA-Zertifikate

Die Inhalte des Subject-DN (Antragsteller) von CA-Zertifikaten setzen sich wahlweise aus den Feldern wie im Kapitel 3.1.1 beschrieben zusammen. Die Felder enthalten Pflichtangaben (mandatory) und ggf. optionale erzeugte Angaben.

Pflichtangaben enthalten folgende Felder:

- Country Name (C)
- Organization Name (O)

- Organizational Unit Name (OU)
- Common Name (CN)

Folgende Felder sind optional:

- StateOrProvinceName (ST)
- Locality (L)
- PostalCode
- StreetAddress (Street)

7.1.5 Namensbeschränkungen

TeleSec ServerPass betreibt keine Sub-CAs mit Namensbeschränkungen.

7.1.6 Objekt-Kennungen (OIDs) für Zertifizierungsrichtlinien

7.1.6.1 Reservierte Zertifikat Policy Identifier

Siehe Kapitel 1.2, 7.1.2.1 und 7.1.6.3.

7.1.6.2 Objekt-Kennungen in Root-CA-Zertifikaten

Die Root-CA-Zertifikate enthalten keine certificatePolicies Erweiterung.

7.1.6.3 Sub-CA Zertifikate

TeleSec ServerPass Class 2 CA

Der TSP verwendet in dem Sub-CA-Zertifikat „TeleSec ServerPass Class 2 CA“, welches unter einer öffentlichen Root ausgestellt wurde, die Policy-OIDs “anyPolicy” identifier (2.5.29.32.0).

TeleSec ServerPass Extended Validation Class 3 CA

Der TSP verwendet in dem Sub-CA-Zertifikat „TeleSec ServerPass Extended Validation Class 3 CA“, welches unter einer öffentlichen Root ausgestellt wurde, die Policy-OIDs “anyPolicy” identifier (2.5.29.32.0).

7.1.6.4 Objekt-Kennungen in Endteilnehmer Zertifikaten

Ein für einen Endteilnehmer ausgestelltes Zertifikat enthält eine der nachfolgende certificatePolicies-Erweiterung:

Policy-OID 2.23.140.1.1

Wird in einem Zertifikat die Policy-OID **2.23.140.1.1** EV (extended validated-Zertifikat) verwendet, müssen zwingend folgende Felder des Subject DN ausgefüllt sein: organizationName, localityName, stateOrProvinceName (falls ein sinnvoller Wert existiert, z.B. Bundesland in Deutschland), commonName und countryName

Policy-OID 2.23.140.1.2.1

Wird in einem Zertifikat die Policy-OID **2.23.140.1.2.1** DV (Domain validated-Zertifikat) verwendet, muss zwingend das folgende Feld des Subject DN ausgefüllt sein: commonName

Die Felder organizationName, localityName, stateOrProvinceName, postalCode, StreetAddress und countryName werden nicht verwendet.

Policy-OID 2.23.140.1.2.2

Wird in einem Zertifikat die Policy-OID 2.23.140.1.2.2 OV (Organization validated-Zertifikat) verwendet, müssen zwingend folgende Felder des Subject DN ausgefüllt sein: organizationName, localityName, stateOrProvinceName (falls ein sinnvoller Wert existiert, z.B. Bundesland in Deutschland), commonName und countryName.

Die Policy-OID **2.23.140.1.2.3** wird nicht verwendet, da keine IV (Individual validated-Zertifikate) ausgestellt werden.

Öffentliche Geräte-Zertifikate verwenden die Policy OID 2.23.140.1.2.2 um zuzusichern, dass das öffentliche Geräte-Zertifikat und dessen Management während seines Lebenszyklus die Anforderungen der [CABF-BR] erfüllen.

7.1.7 Verwendung der Erweiterung der Richtlinieneinschränkungen

Nicht anwendbar.

7.1.8 Syntax und Semantik von Richtlinienkennungen

Die Endteilnehmer-Zertifikate enthalten eine URL auf den Ablageort des CPS. Ältere Versionen werden in entsprechender Ablage (Repository) abgelegt.

7.1.9 Verarbeitungssemantik für die Erweiterung „Kritische Zertifikats-Richtlinien“ (Critical Certificate Policies)

Nicht anwendbar.

7.1.10 Subject-DN Serial Number (SN)

Zertifikate mit gleichlautendem Subject-DN werden ausschließlich für einen Kunden ausgestellt. Neuen Zertifikaten anderer Kunden mit einem bereits verwendeten Subject-DN wird zur Unterscheidung im Subject-DN eine eindeutige Serial Number (SN) hinzugefügt.

7.2 Sperrlistenprofil

Die von der Zertifizierungsstelle ausgestellten Sperrlisten entsprechen folgenden Anforderungen:

- [RFC 5280]
- [X.509] Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, Recommendation X.509 (08/05), Recommendation X.509 (2005) Corrigendum 1 (01/07)

Zertifikatssperrlisten müssen mindestens die in Tabelle 7 aufgeführten Inhalte aufweisen.

Tabelle 7: Sperrlistenattribute nach X509.v2

Feld	**Wert oder Wertbeschränkung**
Version:	Sperrlistenversion (siehe Kapitel 7.2.1)
Aussteller:	(siehe Kapitel 7.1.4)
Gültig ab:	Zeitbasis Koordinierte Weltzeit (UTC). Gemäß RFC 5280 kodiert.
Nächste Aktualisierung (NextUpdate):	Datum und Uhrzeit der nächsten geplanten Veröffentlichung.
Signaturalgorithmus:	1.2.840.113549.1.1.11 / sha256WithRSAEncryption(11)
Gesperrte Zertifikate:	Liste der gesperrten Zertifikate inkl. Seriennummer mit Sperrdatum- und zeitpunkt des gesperrten Zertifikats.
Erweiterungen	
Stellenschlüsselkennung (AuthorityKeyIdentifier):	Sinngemäß gilt Kapitel 7.2.2.1
Sperrlistennummer (cRLNumber):	Fortlaufende Nummer der Zertifikatssperrliste (Kapitel 7.2.2.2).
Sperrgrund:	(optional) Kodierung des Sperrgrunds nach RFC 5280, siehe hierzu Kapitel 7.2.2.3
CRL enthält abgelaufene Zertifikate (ExpiredCertsOnCRL)	Sinngemäß gilt Kapitel 7.2.2.4

7.2.1 Versionsnummer(n)

Die Zertifizierungsstelle unterstützt Zertifikatssperrlisten im Format X.509 Version 2, die den die Anforderungen gemäß RFC 5280 erfüllen.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

7.2.2.1 Erweiterung „Stellenschlüsselkennung “ (authorityKeyIdentifier)

Die Sperrlisten enthalten die Erweiterung „Stellenschlüsselkennung“ wie in Kapitel 7.1.2.6 beschrieben.

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.2.2.2 Erweiterung „Sperrlistennummer“ (cRLNumber)

Die Sperrlisten enthalten die Erweiterung „Sperrlistennummer“ als fortlaufende Seriennummer der Sperrliste.

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.2.2.3 Erweiterung “Sperrgrund”

Bei der Sperrung von Zertifikaten muss zwingend ein Sperrgrund angegeben werden. Nach Tabelle 8 sind folgende Sperrgründe implementiert:

Tabelle 8: Erweiterung „Sperrgrund“

Eingabewert auf Webseite:	**Sperrgründe nach RFC 5280:**	**Wert:**
Nicht spezifiziert; Falsche Zertifikatsverwendung ("Zertifikatsmissbrauch")	unspecified	
Schlüssel kompromittiert	keyCompromise	1
CA kompromittiert	cACompromise	2
Angaben im Zertifikat nicht mehr aktuell oder falsch	affiliationChanged	3
Zertifikat wird nicht mehr benötigt	superseded	4
Geschäftsaufgabe	cessationOfOperation	5
Rechte wurden entzogen (Recht auf Nutzung des Domainnamens erloschen)	privilegeWithdrawn	9

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.2.2.4 CRL enthält abgelaufene Zertifikate (ExpiredCertsOnCRL)

Die Sperrlisten enthalten auch abgelaufene Zertifikate (ExpiredCertsOnCRL).

Der Risikowert dieser Erweiterung ist als „unkritisch“ gesetzt.

7.3 OCSP-Profil

OCSP (Online Certificate Status Protocol) stellt auf gleichnamigem Protokoll einen Validierungsdienst zur Verfügung, mit dessen Hilfe dem Vertrauende Dritten eine zeitgerechte Information zum Sperrstatus von Endteilnehmer-Zertifikaten übermittelt wird.

Der eingesetzte OCSP-Dienst erfüllt die Anforderungen des RFC 6960.

7.3.1 OCSP-Erweiterungen

Das von der Zertifizierungsstelle ausgestellte OCSP-Zertifikat enthält das Attribut „Erweiterter Schlüsselverwendung“ mit der OID „1.3.6.1.5.5.7.3.9“ (OCSP noCheck, id-pkix-ocsp-nocheck), d.h. das OCSP-Zertifikat wird nicht validiert.

Die ArchiveCutOff Erweiterung wird nicht verwendet.

8 COMPLIANCE-AUDITS UND ANDERE PRÜFUNGEN

Die Stellen, die einem Audit, einer Überprüfung oder einer Untersuchung unterzogen werden, müssen das Trust Center und/oder einen beauftragten Dritten unterstützen.

Weiterhin ist das Trust Center berechtigt, die Durchführung dieser Audits, Überprüfungen und Untersuchungen auf Dritte (Kapitel 8.2) zu übertragen.

TeleSec ServerPass Standard und SAN/UCC:

Die Trust Center Prozesse werden durch unabhängige Dritte einer regelmäßigen jährlichen Prüfung (ETSI EN 319411-1, policy OVCP) unterzogen. Das Trust Center führt zusätzlich in regelmäßigen Abständen Selbstaufsichtsmaßnahmen durch (siehe auch Kapitel 8.1).

TeleSec ServerPass EV/EV SAN:

Die Trust Center Prozesse werden regelmäßig durch unabhängige Dritte einer regelmäßigen jährlichen Prüfung (ETSI EN 319411-1 policy EVCP, ETSI EN 319 411-2 QCP-w) unterzogen. Das Trust Center führt zusätzlich in regelmäßigen Abständen Selbstaufsichtsmaßnahmen durch (siehe auch Kapitel 8.1).

Zertifizierungsgegenstand sind alle Prozesse, die zur Beantragung, Ausstellung, Wiederausstellung, Sperrung und Erneuerung von Endteilnehmer-Zertifikaten dienen.

8.1 Intervall und Grund von Prüfungen

Compliance-Audits finden mindestens jährlich und zusätzlich bei Bedarf (Kapitel 8) statt und werden auf Kosten der überprüften Stelle durchgeführt. Der Beginn dieser Maßnahme ist mindestens eine Woche vorher schriftlich anzukündigen. Audits werden über eine ununterbrochene Folge von Auditperioden durchgeführt, deren Zeitraum die Dauer von einem Jahr nicht überschreitet.

Selbstaufsichtsmaßnahmen (Quality Assessments), die die Servicequalität sicherstellen, finden regelmäßig, jedoch mindestens vierteljährlich, statt. Es werden mindestens 3 (drei) Prozent der in diesem Zeitraum ausgestellten Zertifikate, aber in jedem Fall 1 ausgestelltes Zertifikat betrachtet, wobei die Auswahl zufällig erfolgt. Es wird immer der Zeitraum, der auf die Periode des vorangegangenen Selfassessments folgt, für die Auswahl herangezogen.

8.2 Identität/Qualifikation des Prüfers

Die Trust Center-spezifischen Compliance-Audits werden von qualifizierten Mitarbeitern der DT Security GmbH oder einem Dritten (z.B. qualifiziertes Unternehmen wie TÜV IT) durchgeführt, die Erfahrung in den Bereichen Public-Key-Infrastructure-Technologie, Sicherheits-Auditing und Verfahren und Hilfsmittel der Informationssicherheit vorweisen können.

Für Auditoren, welche im Trust Center ein Audit auf Anforderung eines oder mehrerer Anwendungssoftwareanbieter durchführen, gelten besondere Anforderungen. Für ServerPass beauftragt das Trust Center einen Auditor einer für die IT-Sicherheit akkreditierten Zertifizierungsstelle. Dadurch ist die Einhaltung der besonderen Anforderungen (z.B. Qualifikation, Unabhängigkeit) an den Auditor gewährleistet.

8.3 Beziehung des Prüfers zur prüfenden Stelle

Beim Prüfer für die ETSI-Zertifizierungen handelt es sich um einen unabhängigen und qualifizierten Auditor (z.B. Wirtschaftsprüfer, Gutachter).

Selbstaufsichtsmaßnahmen (Quality Assessments) werden von dafür qualifizierten internen Auditoren der DT Security GmbH durchgeführt.

8.4 Abgedeckte Bereiche der Prüfung

Zielsetzung der Überprüfung ist die Umsetzung dieses Dokuments. Es sind alle Prozesse zu prüfen, die mit der Lebenszyklusverwaltung von Zertifikaten in Verbindung stehen:

- Identitätsprüfungen der Endteilnehmer,
- Zertifikatsbeauftragungsverfahren,
- Bearbeitung von Zertifikatsaufträgen,
- Zertifikatserneuerung/ Re-Zertifizierung (nur TeleSec ServerPass Standard, SAN/UCC),
- Zertifikatssperrungen,
- Zutrittsschutz,
- Berechtigungs- und Rollenkonzept,
- Einbruchshemmende Maßnahmen,
- Personal

In jedem Fall wird nach den jeweils gültigen Versionen der folgenden Audit-Kriterien geprüft:

ETSI EN 319 411-1 policy OVCP.

TeleSec ServerPass EV/EV SAN:

Des Weiteren decken die Prüfungen die (ETSI EN 319411-1 policy EVCP) genannten, für die Ausgabe von Extended Validation Zertifikaten besonders zu beachtende Punkte ab.

Weiterhin ein jährliches Vollaudit nach ETSI EN 319 411-2, policy QCP-w für die Ausstellung von eIDAS konformen qualifizierten Zertifikaten für Website-Authentifizierung.

8.4.1 Risikobewertung und Sicherheitsplan

Das Trust Center führt jährlich eine Risikobewertung durch, welches u.a. auch das Produkt ServerPass abdeckt.

Die Überprüfung beinhaltet zumindest die folgenden Punkte:

1) Identifikation vorhersehbarer externer, als auch interner Gefährdungen (d.h. insbesondere die zu Grunde liegenden Schwachstellen), welche
    1. zu unbefugten Zugriffen auf relevante Daten oder Systeme,
    2. zur Weitergabe oder einem Missbrauch von relevanten Daten,
    3. zu Veränderungen oder Zerstörung von relevanten Daten,
    4. zur Beeinträchtigung, Störung oder Ausfall von Teilen oder des gesamten Zertifikatsverwaltungsprozesses

    führen können.
2) Beurteilung der Eintrittswahrscheinlichkeit und der daraus resultierenden potenziellen Schäden (d.h. Schadenshöhe) durch das Ausnutzten einer Schwachstelle. Dabei ist der besondere Schutzbedarf der Zertifikatsdaten und des Zertifikatsverwaltungsprozesses zu berücksichtigen.

3) Beurteilung der Wirksamkeit und Angemessenheit der getroffenen Gegenmaßnahmen (z.B. Richtlinien, Verfahren, eingesetzte Sicherheits-Systeme, Technologien, Versicherungen) welche die Gefährdung beseitigen oder das Risiko minimieren.

Basierend auf der Risikobewertung hat das Trust Center einen Sicherheitsplan entwickelt, der regelmäßig überprüft und bei Bedarf angepasst wird. Der Sicherheitsplan besteht aus Verfahren, Maßnahmen und Produkten um die Bewertung und Management der während der Risikobewertung identifizierten Risiken zu unterstützen. Der Sicherheitsplan enthält entsprechend der Sensibilität der Daten und des Zertifikatsverwaltungsprozesses administrative, organisatorische, technische und physische Sicherheitsmaßnahmen.

8.5 Maßnahmen zur Beseitigung von Mängeln oder Defiziten

Werden bei einem Compliance-Audit von einem Prüfer schwerwiegende Mängel oder Fehler bei dem Betreiber der Zertifizierungsstelle festgestellt, wird darüber entschieden, welche Korrekturmaßnahmen zu treffen sind. Der Leiter Trust Center entscheidet zusammen mit dem Prüfer über geeignete Maßnahmen, deren Umsetzung in einem wirtschaftlich angemessenen Zeitraum durch zu führen sind. Bei schweren sicherheitskritischen Mängeln muss innerhalb von 10 Tagen ein Korrekturplan erstellt und die Abweichung behoben werden. Bei weniger schwerwiegenden Defiziten entscheidet der Leiter Trust Center über den Zeitrahmen der Behebung.

8.6 Mitteilung der Ergebnisse

Die Ergebnisse der Prüfung werden in einem vom Prüfer erstellten Bericht dokumentiert und dem Trust Center übergeben.

Das Trust Center behält sich vor, Ergebnisse bzw. Teilergebnisse zu veröffentlichen, wenn Missbrauch stattfand oder bei Schädigung des Ansehens der DT Security GmbH.

Auditberichte, die auf Anforderung eines oder mehrerer Anwendungssoftwareanbieter abgelegt werden, welche ein Stammzertifizierungsstellenzertifikat des Trust Centers einbetten, müssen spätestens drei Monate nach Ablauf der jeweiligen Auditperiode veröffentlicht werden.

Für ServerPass werden die geforderten Audits abgelegt. Die zugehörigen Berichte werden auf der Internetseite https://www.telesec.de/de/service/downloads/pki-repository/ im Menü „Audit Attestations and Certifications -> Certifications -> ETSI-Zertifikate TeleSec ServerPass“ und „Audit Attestations and Certifications -> Certifications -> eIDAS – Konformitätsbewertungen für Vertrauensdiensteanbieter“ veröffentlicht.

8.7 Selbst-Audits

Es werden Selbst-Audits, wie in Kapitel 8.1 beschrieben, durchgeführt.

9 SONSTIGE GESCHÄFTLICHE UND RECHTLICHE BESTIMMUNGEN

9.1 Entgelte

9.1.1 Entgelte für die Ausstellung oder Erneuerung von Zertifikaten

Die Zertifizierungsstelle ist berechtigt, für das Ausstellen, Erneuern und Verwalten von Endteilnehmer-Zertifikaten Entgelte zu berechnen. Die Preise sind in den geltenden „Leistungsbeschreibung und Preise TeleSec ServerPass“ geregelt.

9.1.2 Entgelte für den Zugriff auf Zertifikate

Das Trust Center berechnet für den Zugriff auf Zertifikate im Verzeichnisdienst von TeleSec ServerPass keine Entgelte. Das Trust Center gestattet Dritten, die selbst Produkte und Dienstleistungen vermarkten, nur nach vorheriger ausdrücklicher schriftlicher Genehmigung den Zugriff und Abruf von Zertifikaten.

Dritten ist es nur nach vorheriger, ausdrücklicher schriftlicher Genehmigung gestattet, die vom Trust Center öffentlich zur Verfügung gestellten Zertifikate und Statusinformationen selbst zu vermarkten oder zur Vermarktung anzubieten.

9.1.3 Entgelte für den Zugriff auf Sperr- oder Statusinformationen

Das Trust Center berechnet für den Zugriff auf Sperr- oder Statusinformationen für die unter den Geltungsbereich dieses Dokumentes fallenden relevanten Anteile keine Entgelte. Das Trust Center gestattet Dritten, die selbst Produkte und Dienstleistungen vermarkten, nur nach vorheriger ausdrücklicher schriftlicher Genehmigung den Zugriff auf Sperr- und Statusinformationen von Zertifikaten.

Dritten ist es nur nach vorheriger, ausdrücklicher schriftlicher Genehmigung gestattet, die vom Trust Center öffentlich zur Verfügung gestellten Zertifikate und Statusinformationen selbst zu vermarkten oder zur Vermarktung anzubieten.

9.1.4 Entgelte für andere Leistungen

Das Trust Center berechnet keine Entgelte für den Abruf dieses Dokuments und der damit verbundenen einfachen Betrachtung.

Jede andere Nutzung, z.B. Vervielfältigung, Änderung oder Herstellung eines abgeleiteten Dokuments, bedarf der vorherigen schriftlichen Genehmigung der Stelle (Kapitel 1.5.1, 9.5.2), die das Urheberrecht des Dokuments besitzt.

9.1.5 Erstattung von Entgelten

Die Erstattung von Entgelten durch die DT Security GmbH erfolgt auf Basis der gesetzlichen Regelungen des deutschen Rechts. Detaillierter Regelungen finden Sie im Dokument „Allgemeine Geschäftsbedingungen TeleSec-ServerPass“[AGB].

9.2 Finanzielle Verantwortlichkeiten

Die finanziellen Verantwortlichkeiten werden in den Allgemeinen Geschäftsbedingungen TeleSec-ServerPass festgelegt.

9.2.1 Versicherungsschutz

Die DT Security GmbH ist in das DTAG Haftpflicht-Konzernversicherungsprogramm integriert. Der Haftpflichtversicherungsschutz geht weit über die in den Anforderungen gewünschte Höhe des Versicherungsschutzes hinaus.

Es besteht eine zusätzliche Versicherung über die nach eIDAS geforderte Deckungsvorsorge (2,5 Mio. pro Schadensereignis).

9.2.2 Sonstige finanzielle Mittel

Nicht anwendbar.

9.2.3 Versicherungs- oder Gewährleistungsschutz für Endteilnehmer

Nicht anwendbar.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Umfang von vertraulichen Informationen

Unter vertraulichen Informationen werden alle Informationen von PKI-Beteiligten (siehe Kapitel 1.3.2 und 1.3.3) des TSP eingestuft, die nicht unter Kapitel 9.3.2 fallen.

9.3.2 Umfang von nicht vertraulichen Informationen

Unter nicht vertraulichen Informationen werden alle impliziten und expliziten Informationen des TSP eingestuft, die in ausgegebenen Zertifikaten, Sperrlisten, Statusinformationen enthalten sind oder davon abgeleitet werden können.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Die Verantwortlichkeit für den Schutz der vertraulichen Informationen sowie über die Einhaltung der datenschutzrechtlichen Bestimmungen liegt beim Trust Center als PKI-Diensteanbieter.

9.4 Schutz von personenbezogenen Daten (Datenschutz)

Die Punkte Datenschutz und Datensicherheit sind in den Allgemeinen Geschäftsbedingungen TeleSec-ServerPass [AGB] beschrieben.

9.4.1 Datenschutzkonzept

Innerhalb des TSP werden zur Leistungserbringung personenbezogene Daten elektronisch gespeichert und verarbeitet. Entsprechend den Konzernvorgaben wurde für den TSP ein Datenschutzkonzept erstellt. Dieses Datenschutzkonzept fasst die datenschutzrelevanten Aspekte um den PKI-Dienst zusammen.

Das Datenschutzkonzept kann in Auszügen auf Anforderung bereitgestellt werden.

9.4.2 Vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.1.

9.4.3 Nicht vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.2.

9.4.4 Verantwortung für den Schutz vertraulicher Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kapitel 9.3.3.

9.4.5 Mitteilung und Zustimmung zur Nutzung vertraulicher Daten

Der Zertifikatsauftraggeber stimmt der Nutzung von personenbezogenen Daten durch eine CA oder RA zu, soweit dies zur Leistungserbringung erforderlich ist.

Ferner dürfen alle Informationen veröffentlicht werden, die nach Kapitel 9.4.3 als nicht vertraulich behandelt werden.

9.4.6 Offenlegung gemäß gerichtlicher oder verwaltungsmäßiger Prozesse

Die Verpflichtung zur Geheimhaltung der vertraulichen Informationen oder personenbezogener Daten entfällt, soweit die Offenlegung kraft Gesetzes oder kraft Entscheidung eines Gerichtes oder einer Verwaltungsbehörde angeordnet worden ist bzw. zur Durchsetzung von Rechtsansprüchen dient. Sobald Anhaltspunkte für die Einleitung eines gerichtlichen oder behördlichen Verfahrens bestehen, die zur Offenlegung vertraulicher oder privater Informationen führen könnten, wird die an dem Verfahren beteiligte Vertragspartei die andere Vertragspartei hierüber unter Beachtung der gesetzlichen Bestimmungen informieren.

9.4.7 Andere Umstände zur Offenlegung von Daten

Nicht anwendbar.

9.5 Rechte des geistigen Eigentums (Urheberrecht)

Die nachfolgenden Kapitel 9.5.1 bis 9.5.4 gelten für geistige Eigentumsrechte von Endteilnehmern und Vertrauenden Dritten.

9.5.1 Eigentumsrechte an Zertifikaten und Sperrungsinformationen

Die Zertifizierungsstellebehält sich jegliche geistigen Eigentumsrechte an Zertifikaten, Sperrungs- oder Statusinformationen, öffentlich zugängliche Verzeichnisdienste und Datenbanken mit den ihnen enthaltenen Informationen vor, die die TeleSec ServerPass CA ausstellt bzw. verwaltet.

Sofern Zertifikate und deren Inhalte die Herkunft dieser Zertifikatshierarchie vollständig wiedergegeben und nicht verändert werden, erteilt die Zertifizierungsstelle die Zustimmung, Zertifikate auf nichtausschließlicher und entgeltfreier Basis zu vervielfältigen und zu publizieren.

Unter Voraussetzung, dass die Nutzung von Sperrungs- oder Statusinformationen und deren Inhalte, die Herkunft dieser Zertifikatshierarchie vollständig wiedergegeben und nicht verändert werden, erteilt die Zertifizierungsstelle ihre Zustimmung, Sperrlisten und Statusinformationen auf nichtausschließlicher und entgeltfreier Basis zu vervielfältigen und zu publizieren, insbesondere an Vertrauende Dritte.

9.5.2 Eigentumsrechte dieses CPS

Dieses Dokument ist urheberrechtlich geschützt, alle geistigen Eigentumsrechte obliegen der DT Security GmbH. Jegliche andere Nutzung (z.B. Vervielfältigung, Verwendung von Texten und Bildern, Änderung oder Erzeugung eines vergleichbaren oder abgeleiteten Dokuments, Weitergabe an Personen ohne Interesse an dem in diesem Dokument beschriebenem Dienst), auch auszugsweise, bedarf der vorherige ausdrücklichen schriftliche Genehmigung des Herausgebers dieses Dokuments (siehe Kapitel 1.5.1).

9.5.3 Eigentumsrechte an Namen

Der Endteilnehmer behält, sofern zutreffend, alle Rechte an Namen oder Marken, die im Zertifikat enthalten sind, sofern das Zertifikat einen eindeutigen Namen beinhaltet.

9.5.4 Eigentumsrechte an Schlüsseln und Schlüsselmaterial

Die geistigen Eigentumsrechte von Schlüsselmaterial der CA- verbleiben bei der DT Security GmbH, ungeachtet des Mediums, auf denen sie gespeichert sind. Kopien von CA-Zertifikate dürfen vervielfältigt werden, um diese in vertrauenswürdige Hardware- und Software-Komponenten zu integrieren.

Die geistigen Eigentumsrechte an den Zertifikaten und der ARL verbleiben bei der DT Security GmbH.

9.6 Zusicherungen und Gewährleistungen

9.6.1 Zusicherungen und Gewährleistungen der Zertifizierungsstelle

Der TSP übernimmt sowohl die Verantwortung für alle Aspekte der Bereitstellung des Zertifizierungsdienstes als auch für die Tätigkeiten, die an Unterauftragnehmer ausgelagert werden. Der TSP hat die Verantwortlichkeiten klar geregelt und geeignete Vorkehrungen getroffen, um Kontrollen durch die Zertifizierungsinstanz bei Dritten durchführen zu dürfen.

Die Zertifizierungsstelle stellt sicher, dass die Sicherheit der Informationen beibehalten wird, auch wenn die Tätigkeiten der Zertifizierungsstelle an andere Organisationen ausgelagert wird.

Die Zertifizierungsinstanz verfügt über eine dokumentierte Vereinbarung und ein aktuelles Vertragsverhältnis, die die Bereitstellung des PKI-Dienstes hinsichtlich Zulieferung, Ausgliederung von Betriebsfunktionen (Outsourcing) oder andere Vereinbarungen mit Dritten unterstützt.

Ebenfalls gelten die entsprechenden Regelungen „Delegierung von Tätigkeiten“ der [CABF-BR].

Der TSP verpflichtet sich dafür Sorge zu tragen,

- dass keine unrichtigen Angaben in Zertifikate aufgenommen werden, die den Registrierungsstellen, die den Zertifikatsauftrag genehmigen oder das Zertifikat ausstellen, bekannt sind oder von ihnen stammen,
- dass keine Fehler in Zertifikaten einfließen, die vom Personal der Registrierungsstellen, die den Zertifikatsauftrag genehmigen oder das Zertifikat ausstellen, gemacht wurden und auf unsachgemäße und sorglose Zertifikatserzeugung und Verwaltung zurück zu führen sind,
- dass alle Zertifikate den Anforderungen dieses Dokuments genügen und

- dass die Sperrfunktionalitäten und die Nutzung der CA-Datenbank (Verzeichnisdienst, OCSP-Responder) allen wesentlichen Anforderungen des geltenden CPS erfüllen.

Weiterhin wird zugesichert, dass zum Zeitpunkt der Ausstellung eines SSL/TLS Zertifikates:

1) eine definierte Prozedur existiert um sicherzustellen, dass der Antragsteller das Recht hat, die im Zertifikat benannten Domains und/oder IP-Adressen zu verwenden. Alternativ ist er über eine entsprechende Vollmacht autorisiert, welche von einer Person oder einer Organisation ausgestellt wurde, welche das Recht zur Verwendung hat.
2) die unter 1) genannte Prozedur befolgt wird und
3) das unter 1) benannte Verfahren in diesem CPS detailliert spezifiziert wird.
4) eine definierte Prozedur befolgt wird, um sicherzustellen, dass der im Zertifikat benannte Zertifikatsnehmer (Subjekt) die Ausstellung des Zertifikates genehmigt hat, sowie, dass der Repräsentant des Antragstellers berechtigt ist, den Antrag zu stellen.
5) die unter 4) genannte Prozedur befolgt wird und
6) das unter 4) benannte Verfahren in diesem CPS detailliert spezifiziert wird.
7) eine definierte Prozedur befolgt wird, um zu prüfen, dass mit Ausnahme des OU-Feldes im subject DN alle im Zertifikat enthaltenen Informationen korrekt sind
8) die unter 7) genannte Prozedur befolgt wird und
9) das unter 7) benannte Verfahren in diesem CPS detailliert spezifiziert wird.
10) eine definierte Prozedur befolgt wird, um die Wahrscheinlichkeit zu minimieren, dass das OU-Feld des subject DN irreführende Informationen enthält
11) die unter 10) genannte Prozedur befolgt wird und
12) das unter 10) benannte Verfahren in diesem CPS detailliert spezifiziert wird.

Außerdem sichert das Trust Center zu, dass im Falle, dass das auszustellende SSL/TLS Zertifikat Informationen zur Identität des Zertifikatsnehmer enthält

13) eine definierte Prozedur zur Überprüfung der angegebenen Identität existiert und befolgt wird, welche die Anforderungen der zum Zeitpunkt der Zertifikatsaustellung gültigen Version der [CABF-BR] Kapitel 9.2.4 und 11.2 erfüllt.
14) das unter 13) benannte Verfahren in diesem CPS detailliert spezifiziert wird.

Der TSP sichert weiterhin zu, dass

15) falls der Zertifikatsnehmer ein Konzernunternehmen (affilate) ist, der Repräsentant des Antragstellers vor der Ausstellung eines Zertifikates die Nutzungsbedingungen akzeptieren muss.
16) falls der Zertifikatsnehmer kein Konzernunternehmen (affiliate) ist, der Antragsteller mit der DT Security GmbH die "Allgemeinen Geschäftsbedingungen TeleSec-ServerPass" und ServerPass Leistungen und Nutzungsbedingungen in einer rechtlich durchsetzbaren Form vereinbart.
17) ein öffentlich zugängliches Verzeichnis betrieben wird, welches Statusinformationen zu Zertifikaten enthält. Dieses Verzeichnis ist 24 x 7 verfügbar.
18) die ausgestellten Zertifikate aus allen in den [CABF-BR] aufgeführten Gründen sperren wird.
19) bei einer Kenntnisnahme der Zertifizierungsstelle über einen Sperrgrund die betroffenen Zertifikate fristgerecht sperren wird.

9.6.2 Zusicherungen und Gewährleistungen der Registrierungsstelle (RA)

Alle Registrierungsstellen verpflichten sich:

- keine unrichtigen Angaben in Zertifikaten aufzunehmen, die den Registrierungsstellen, die den Zertifikatsauftrag genehmigen oder das Zertifikat ausstellen, bekannt sind oder von ihnen stammen,
- dass keine Fehler in Zertifikaten enthalten sind, die vom Personal der Registrierungsstellen, die den Zertifikatsauftrag genehmigen oder das Zertifikat ausstellen,

gemacht wurden und auf unsachgemäße und sorglose Zertifikatserzeugung und Verwaltung zurück zu führen sind,
- die rechtlichen Konsequenzen zu tragen, die durch die Nichteinhaltung der beschriebenen Pflichten entstehen,
- dass alle Zertifikate den wesentlichen Anforderungen dieses Dokuments genügen.

9.6.3 Zusicherungen und Gewährleistungen des Endteilnehmers

Endteilnehmer verpflichten sich,

- einen Zertifikatsrequest (PKCS#10) zu generieren, der den technischen Anforderungen aus Kap. 6.1.6 entspricht,
- ihren privaten Schlüssel vor unberechtigtem Zugriff durch Dritte zu schützen. Im Falle von privaten Schlüsseln von juristischen Personen erfolgt der Schutz durch autorisierte Personen,
- das Endteilnehmer-Zertifikat nur bestimmungsgemäß und nicht missbräuchlich zu benutzen,
- dass das Zertifikat gültig (nicht abgelaufen und nicht gesperrt) verwendet wird,
- zu überprüfen, dass die im Endteilnehmer-Zertifikat aufgenommenen Zertifikatsinhalte des Subject-DN der Wahrheit entsprechen. Im Falle von juristischen Personen erfolgt die Prüfung der Zertifikatsinhalte durch autorisierte Personen,
- die rechtlichen Konsequenzen zu tragen, die durch die Nichteinhaltung des vorliegenden CPS beschriebenen Pflichten entstehen,
- bei Verlust oder Verdacht der Kompromittierung des privaten Schlüssels eine Sperrung des entsprechenden Endteilnehmer-Zertifikat selbst durchzuführen oder die Registrierungsstell zu beauftragen,
- bei Kompromittierung des privaten Schlüssels, die Verwendung dieses privaten Schlüssels unmittelbar und dauerhaft einzustellen,
- dass das ausgestellte Zertifikat ausschließlich für autorisierte und legale Zwecke die, diesem CPS entsprechen, verwendet wird und nicht den Regelungen dieser Erklärung widersprechen,
- dass alle, im Zertifikats-Auftrag gemachten Angaben, die zur Ausstellung des Zertifikats führten, der Wahrheit entsprechen,
- dass der Endteilnehmer tatsächlich ein Endteilnehmer ist und mit seinem privaten Schlüssel, dem der im Zertifikat enthaltene öffentliche Schlüssel zugeordnet ist, keine CA-Funktionalitäten durchführt wie z.B. Signatur von Zertifikaten oder Sperrlisten.
- dass Endteilnehmer-Zertifikat unverzüglich zu sperren und damit als ungültig zu erklären, wenn die Zertifikatsangaben nicht mehr stimmen, der private Schlüssel abhanden gekommen ist, gestohlen wurde, eine Kompromittierung vorliegt, oder ein sonstiger Missbrauch vermutet wird.

Hinweis: Die DT Security GmbH behält sich vor, weiteren Pflichten, Zusicherungen, Zusagen und Gewährleistungen gegenüber dem Endteilnehmers abzuschließen.

9.6.4 Zusicherungen und Gewährleistungen vertrauender Dritter

Vertrauende Dritte müssen selbst über hinreichende Informationen und Kenntnisse verfügen, um den Umgang mit Zertifikaten und dessen Validierung bewerten zu können. Der vertrauende Dritte ist selbst für seine Entscheidungsfindung verantwortlich, ob die die zur Verfügung gestellten Informationen zuverlässig und vertrauensvoll sind.

Vertrauende Dritte sollten

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

9.6.5 Zusicherungen und Gewährleistungen anderer Teilnehmer

Nicht anwendbar.

9.7 Haftungsausschluss

Der Haftungsausschluss ist in den geltenden Allgemeinen Geschäftsbedingungen TeleSec-ServerPass [AGB] geregelt.

9.8 Haftungsbeschränkungen

Für Schäden aus der Verletzung von Leben, Körper und Gesundheit sowie für Schäden, die auf eine vorsätzliche Pflichtverletzung zurückzuführen sind, haftet die Zertifizierungsstelle unbegrenzt. Im Übrigen wird die Haftung für Schäden, die auf einer fahrlässigen Pflichtverletzung beruhen in den Allgemeinen Geschäftsbedingungen TeleSec-ServerPass [AGB] oder einzelvertraglich geregelt.

9.9 Schadensersatz

Schadensersatz ist in den geltenden Allgemeinen Geschäftsbedingungen TeleSec-ServerPass [AGB] geregelt.

9.10 Laufzeit und Beendigung

9.10.1 Laufzeit

Das CPS tritt mit der Veröffentlichung auf den Trust Center Webseiten in Kraft.

Änderungen treten ebenfalls mit der Veröffentlichung auf den öffentlichen Webseiten (siehe Kapitel 2.3) in Kraft.

9.10.2 Beendigung

Dieses CPS bleibt in der jeweils gültigen Version in Kraft, bis sie durch eine neue Version ersetzt wird.

9.10.3 Wirkung der Beendigung und Fortbestand

Bei der Beendigung des Dienstes TeleSec ServerPass bleiben alle Benutzer an die, im CPS enthaltenen Regelungen gebunden, bis das letzte ausgegebene Zertifikat seine Gültigkeit verliert oder gesperrt wird.

9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Falls nicht anders vertraglich vereinbart, werden für individuelle Mitteilungen an die Zertifizierungsstelle die jeweils gültigen Kontaktinformationen (Anschrift, E-Mail etc.) bekannt gegeben.

9.12Änderungen des CPS

Um auf sich ändernde Marktanforderungen, Sicherheitsanforderungen, Gesetzeslagen etc. zu reagieren, behält sich die Zertifizierungsstelle das Recht vor, Änderungen und Anpassungen dieses Dokuments durchzuführen.

9.12.1 Verfahren für Änderungen

Änderungen des CPS können nur vom Trust Center Change Advisory Board durchgeführt werden. Bei jeder offiziellen Änderung erhält dieses Dokument eine neue aufsteigende Versionsnummer und ein Veröffentlichungsdatum.

Änderungen treten unverzüglich mit der Veröffentlichung in Kraft (siehe auch Kapitel 2.3).

Aktualisierte Versionen setzen die vorherigen Dokumentenversionen außer Kraft. Im Falle widersprüchlicher Bestimmungen entscheidet das Trust Center Change Advisory Board über die weitere Vorgehensweise.

9.12.2 Benachrichtigungsverfahren und -zeitraum

Reseller werden über Änderungen informiert und erhalten Gelegenheit innerhalb von sechs Wochen Widerspruch ein zu legen. Erfolgen keine Widersprüche, dann tritt die neue Dokumentenversion wie unter Kapitel 9.12.1 in Kraft. Darüber hinaus gehende Ansprüche auf die Benachrichtigung einzelner Endanwender sind explizit ausgeschlossen.

Falls das Trust Center Change Advisory Board der Ansicht ist, dass gravierende z.B. sicherheitsrelevante Änderungen unverzüglich erforderlich sind, dann tritt das neue CPS unverzüglich mit der Freigabe (siehe Kapitel 9.12.1) in Kraft.

9.13Bestimmungen zur Beilegung von Streitigkeiten

Im Falle von Streitigkeiten führen die Parteien unter Berücksichtigung getroffener Vereinbarungen, Regelungen und geltender Gesetze die Einigung herbei.

9.14Geltendes Recht

Es gilt das Recht der Bundesrepublik Deutschland.

9.15Einhaltung geltenden Rechts

Das vorliegende Dokument unterliegt den geltenden deutschen Gesetzen, Vorschriften, Richtlinien, Verordnungen, Erlassen und Anordnungen, insbesondere den darin beschriebenen Import und Export Bestimmungen von Security-Komponenten (Software, Hardware oder technischer Informationen). Geltende zwingende Gesetze, Vorschriften, Richtlinien, Verordnungen, Erlasse und Anordnungen setzen die entsprechenden Bestimmungen des vorliegenden Dokuments außer Kraft.

9.16Verschiedene Bestimmungen

9.16.1 Vollständiger Vertrag

Nicht anwendbar.

9.16.2 Abtretung

Nicht anwendbar.

9.16.3 Salvatorische Klausel

Sollte eine Bestimmung dieses CPS unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit dieser Erklärung im Übrigen nicht. Statt der unwirksamen und undurchführbaren Bestimmung gilt eine solche Bestimmung als vereinbart, die dem wirtschaftlichen Zweck dieses Dokuments in rechtswirksamer Weise am nächsten kommt. Das Gleiche gilt für die Ergänzung etwaiger Vertragslücken.

9.16.4 Vollstreckung (Rechtsanwaltsgebühren und Rechtsverzicht)

Nicht anwendbar.

9.16.5 Höhere Gewalt

Telekom Security haftet nicht, wenn aufgrund höherer Gewalt die vertragliche Leistung wesentlich erschwert oder die ordnungsgemäße Durchführung des Vertrages zeitweilig behindert wird bzw. unmöglich ist.

9.17 Sonstige Bestimmungen

9.17.1 Barrierefreiheit

Der Zugang zu den TC-Services erfolgt im Wesentlichen browserbasiert. Betriebssysteme bieten hier eine Vielzahl unterschiedlicher Barrierefreiheitsfeatures, um behinderten Personen den Zugriff auf die Web-Portale der Trust Center Services zu erleichtern. Diese kompensieren insbesondere Einschränkungen des Seh- und Hörvermögens, physischen Einschränkungen sowie Wahrnehmungsstörungen (z.B. „Informationen zur Barrierefreiheit für IT-Experten“).

Sollten vorgenannte Maßnahmen nicht ausreichen, bietet das Trust Center darüber hinaus behinderten Menschen zur Unterstützung bei der Beantragung, Akzeptanz und Sperrung von Zertifikaten kostenlosen telefonischen Support.

10MITGELTENDE UNTERLAGEN UND REFERENZEN

10.1Mitgeltende Unterlagen

Tabelle 9: Erweiterung „Mitgeltende Unterlagen“

Referenz / Nr.	Dokumentenbezeichnung	Link
[AGB]	Allgemeine Geschäftsbedingungen TeleSec-ServerPass	https://telesec.de/de/service/downloads/allgemeine-geschaeftsbedingungen/
[PDS]	PKI Disclosure Statement	https://telesec.de/de/service/downloads/pki-repository/

10.2Referenzen

Tabelle 10: Erweiterung „Referenzen“

Referenz	Dokumentenbezeichnung
[BDSG]	Bundesdatenschutzgesetz
[CABF-BR]	Die jeweils aktuell gültige Version des vom CA/Browser Forum (https://cab-forum.org) herausgegebenen Dokumentes „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“.
[CABF-BREV]	Guidelines For The Issuance and Management Of Extended Validation Certificates, The CA/Browser Forum
[ETSI EN TSP]	ETSI EN 319 401, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures
[ETSI EV]	ETSI EN 319 411-1 policy EVCP. „Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates“, European Telecommunications Standards Institute
[ETSI POL]	ETSI EN 319 411-1, policy OVCP. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI QC]	ETSI EN 319 412-5, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[ETSI QCP-w]	ETSI EN 319 411-2, policy QCP-w. 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
[ETSI WEB]	ETSI EN 319 412-4, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations
[PKCS]	RSA Security Inc., RSA Laboratories „Public Key Cryptography Standards“ http://www.rsa.com/rsalabs/
[PKIX]	RFCs und Spezifikationen der IETF Arbeitsgruppe Public Key Infrastructure (X.509)
[RFC2560]	X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol - OCSP
[RFC3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003
[RFC5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC6844]	DNS Certification Authority Authorization (CAA) Resource Record, P. Hallam-Baker, R. Stradling IETF, 2013
[RFC6960]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, S. Santesson et. al., IETF, 2013
[SOGIS]	Senior Officials Group Information Systems Security (https://www.sogis.eu/)
[X.509]	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, Recommendation X.509 (08/05), Recommendation X.509 (2005) Corrigendum 1 (01/07), http://www.itu.int/rec/T-REC-X.509/en/https://www.itu.int/rec/T-REC-X.509/en/

11GLOSSAR

Tabelle 11: Erweiterung „Glossar“

Abkürzung	Beschreibung
Authentifizierung	Prüfung einer Identität an Hand behaupteter Merkmale.
Authority Revocation List (ARL)	Liste, in der gesperrte digitale Zertifikate von Zertifizierungsstellen (CA- und Root-CA) aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats einer Zertifizierungsstelle sollte anhand der ARL überprüft werden, ob dieses noch verwendet werden darf.
Certification Authority Authorization (CAA)	Ein Verfahren, bei dem der Domain-Inhaber im DNS festlegen kann, welche Zertifizierungsstelle(n) für seine Domain(s) Zertifikate ausstellen dürfen.
Certification Authority Revocation List (CARL)	Siehe ARL
Certificate Signing Request (CSR)	Von einem Gerät (z.B. Server) elektronisch erstellt und mit dem privaten Schlüssel signierter Zertifikatsantrag, der in kodierter Form den öffentlichen Schlüssel und die Zertifikatsdaten enthält. Die Syntax wird durch den Standard PKCS#11 beschrieben.
Certificate Policy (CP)	Legt die Richtlinien für die Generierung und Verwaltung von Zertifikaten eines bestimmten Typs fest.
Certificate Revocation List (CRL)	Siehe Sperrliste.
Certificate Transparency	Ein Google-Projekt für Zertifikatstransparenz: Ausgestellte Zertifikate werden in öffentlich überprüfbare, manipulationsgeschützte Logserver geschrieben, um missbräuchlich oder fehlerhaft ausgestellte TLS/SSL-Zertifikate schneller ermitteln und blockieren zu können. Während dem Zertifikatsausstellungsprozess werden erforderliche CT Logserver kontaktiert. Diese wiederum liefern in ihrer Antwort je einen SCT zurück, die dann im Zertifikat hinterlegt werden und nachweisen, dass das Zertifikat auf einem Logserver registriert wurde.
Certification Authority	Siehe Zertifizierungsstelle.
Certification Practice Statement (CPS)	Erklärungen für den Betrieb einer Zertifizierungsstelle. Insbesondere setzt das CPS die Vorgaben und Richtlinien der CP einer Zertifizierungsstelle um.
Cross-Zertifikat	Ein Sub-CA-Zertifikat, das von einem etablierten Root-Zertifikat für ein neues Root-Zertifikat ausgestellt wird, das noch nicht über hohe Marktdurchdringung verfügt. Es stellt sicher, dass die Zertifikats-Validierung erfolgreich verläuft, indem ein alternativer Validierungspfand zu einer zweiten Stammzertifizierungsstelle genutzt wird.
crt.sh	Eine Suchmaschine, um in allen öffentlichen CT-Logs (Certificate Transparency) nach Zertifikaten zu suchen.
Digitale Signatur	Mit einem speziellen mathematischen Verfahren erstellte Prüfsumme. Sichert die Authentizität des Signierenden und die Integrität der Daten.

Digitales Zertifikat	Datensatz, der den Namen einer Person oder eines Systems, deren öffentlichen Schlüssel, gegebenenfalls einige andere Angaben und eine Signatur einer Zertifizierungsstelle enthält.
Distinguished Name	Format, mit dem gemäß dem X.500-Standard eindeutige Namen angegeben werden können. In einem digitalen Zertifikat muss ein DN enthalten sein.
Domain Name Systems	Hierarchischer Verzeichnisdienst, der den Namensraum des Internets verwaltet. Hauptsächlich dient es dazu, Domainnamen in IP-Adressen aufzulösen.
Elektronische Signatur	Siehe digitale Signatur.
Endteilnehmer	Siehe auch Zertifikatsnehmer. Der Begriff Endteilnehmer wird überwiegend im Umfeld X.509 verwendet.
Endteilnehmer-Zertifikat	Ein Zertifikat, welches nicht die Basiseinschränkung (basis constraints) „Zertifizierungstelle“ verwendet, daher selber keine Zertifikate signieren kann.
Geräte-Zertifikat	X.509 V3 Zertifikat, welches im commonName-Feld (CN) des distinguishedName des Zertifikatsnehmers (Subject) und/oder in mindestens einer subjectAltName-Erweiterung entweder einen Hostname oder eine IP-Adresse enthält.
Gültigkeitsdauer	Der Zeitraum vom Ausstellungsdatum (not before) des Zertifikats bis zum Ablaufdatum (not after).
Hardware Security Modul (HSM)	Hardware zur sicheren Erzeugung und Speicherung privater Schlüssel.
Hashwert	In diesem Zusammenhang eine kryptografische Prüfsumme fester Länge (die korrekte Bezeichnung wäre kryptografischer Hashwert). Es soll möglichst unwahrscheinlich sein, aus dem Hashwert die Eingabe berechnen oder mehrere mögliche Eingaben zu dem gleichen Hashwert finden zu können (Hashwert wird synonym zu Fingerprint verwendet). Statt einem gesamten digitalen Dokument wird meist nur ein Hashwert signiert.
Interner Servername	Ein Server-Name (der einen nicht registrierten Domain-Namen enthalten kann oder nicht), der nicht mit dem öffentlichen Domain Name System (DNS) aufgelöst werden kann.
Juristische Person	Eine Gesellschaft, ein Konzern, eine Partnerschaft, Einzelfirma, Treuhandgesellschaft, Regierungsbehörde oder eine andere klagebefugte Rechtspersönlichkeit innerhalb des Rechtssystems eines Landes.
Kompromittierung	Ein privater Schlüssel ist kompromittiert, wenn er Unbefugten bekannt geworden ist oder von diesen genutzt werden kann. Eine Kompromittierung kann etwa die Folge eines kriminellen Angriffs sein.
Kryptografie	Wissenschaft, die sich mit der Verschlüsselung von Daten und verwandten Themen beschäftigt (etwa digitale Signatur).
Latenzzeit	Zeitraum zwischen einer Aktion und dem Eintreten einer verzögerten Reaktion (Verzögerungszeitraum). Bei der Latenzzeit erfolgt die Aktion im Verborgenen und wird erst durch die Reaktion festgestellt.

Lightweight Directory Access Protocol (LDAP)	Protokoll zur Abfrage von Verzeichnissen, welches das deutlich kompliziertere Directory Access Protocol (DAP) in vielen Bereichen verdrängt hat. LDAP bietet mehr Möglichkeiten als HTTP und FTP (etwa das Einrichten eines Kontexts, der über mehrere Anfragen aufrechterhalten werden kann). LDAP wird insbesondere zur Abfrage von digitalen Zertifikaten und Sperrlisten innerhalb von Public-Key-Infrastrukturen verwendet.
Managementsystem für Informationssicherheit (ISMS)	Das „Managementsystem für Informationssicherheit“ (ISMS) ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Der Begriff wird im Standard ISO/IEC 27002 verwendet, ISO/IEC 27001 definiert ein ISMS.
Nutzungsbedingungen (Terms of Use)	Bestimmungen bezüglich der Verwahrung und zugelassenen Verwendungszwecke eines ausgestellten Zertifikats in Übereinstimmung mit den gegebenen Anforderungen, wenn der Antragsteller/Zertifikatnehmer beispielsweise ein verbundenes Unternehmen der Zertifizierungsstelle (CA) ist.
Object Identifier (OID)	Ein eindeutiger alphanumerischer oder numerischer Bezeichner, der unter dem jeweiligen Standard für ein bestimmtes Objekt oder eine Objektklasse der Internationalen Organisation für Normung (ISO) registriert ist.
Online Certificate Status Protocol (OCSP)	Ein Protokoll zur Online-Zertifikatsvalidierung, mit dessen Hilfe die Anwendungssoftware der vertrauenden Seite den Status eines identifizierten Zertifikats bestimmen kann.
OCSP-Responder	Ein Online-Server, der der Zertifizierungsstelle (CA) untersteht und mit deren zentrale Datenablage (Repository) zur Bearbeitung von Zertifikatsstatusanfragen verbunden ist. Siehe auch Online Certificate Status Protocol (OCSP).
Öffentlicher Schlüssel	Der Schlüssel eines Schlüsselpaares, der vom Inhaber des entsprechenden privaten Schlüssels offen gelegt werden darf und der von der vertrauenden Seite verwendet wird, um digitale Signaturen zu verifizieren, die mit dem privaten Schlüssel des Inhabers erstellt wurden, und/oder um Mitteilungen zu verschlüsseln, die nur mit dem zugehörigen privaten Schlüssel des Inhabers entschlüsselt werden können.
Öffentliches Geräte-Zertifikat	Ein Geräte-Zertifikat, welches in der CA-Hierarchie von einer Sub-CA unterhalb eines öffentlichen Root-Zertifikates ausgestellt ist.
Phishing	Angriffsmethode im Internet, um an (geheime) Daten (z.B. PINs, TANs, Passwörter) eines Internetnutzers zu gelangen. Meist werden die Opfer dazu auf gefälschte Webseiten gelockt und zur Eingabe der Daten aufgefordert. Da die Seite auf den ersten Blick offiziellen Charakter hat, ist der Nutzer oft bereit, diese Daten preiszugeben.
Privater Schlüssel	Der Schlüssel eines Schlüsselpaares, der vom Schlüsselpaarinhaber geheim gehalten und verwendet wird, um digitale Signaturen zu erstellen und/oder elektronische Daten und Dateien zu entschlüsseln, die mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden.

Public Key Infrastructure X.509 (PKIX)	Standard der IETF, der alle relevanten Bestandteile einer PKI standardisiert.
Policy	Richtlinien, die das Sicherheitsniveau für die Erzeugung und Verwendung von Zertifikaten festlegen. Es wird zwischen Certificate Policy (CP) und Certification Practice Statement (CPS) unterschieden.
Public Key Infrastruktur	Gesamtheit der Komponenten, Prozesse und Konzepte, die zur Verwendung von Public-Key-Verfahren verwendet werden. Typischerweise besteht eine Public-Key-Infrastruktur aus zentralen Komponenten wie einer Zertifizierungsstelle und einem Verzeichnisdienst und verschiedenen Client-Komponenten.
Registration Authority	Siehe Registrierungsstelle.
Registrierungsstelle(RA)	Komponente, mit der eine Person oder ein System kommunizieren muss, um ein digitales Zertifikat zu erhalten.
Request	Engl. Begriff für Auftrag. In diesem Zusammenhang ist der Zertifikatsauftrag zu verstehen.
Rivest Shamir Adleman (RSA)	Verfahren zur Verschlüsselung, zur digitalen Signatur und zur sicheren Übertragung von Schlüsseln, das nach den drei Kryptografen Rivest, Shamir und Adleman benannt ist.
Root-CA	Siehe Stammzertifizierungsstelle (Root-CA)
Secure Multipurpose Internet Mail Extension (S/MIME)	Secure Multipurpose Internet Mail Extension. Erweiterung des E-Mail-Formats MIME, die Zusätze für kryptografische Dienste beschreibt, welche Authentizität, Integrität und Vertraulichkeit von Nachrichten sicherstellen.
Schlüssel	Ein Schlüssel bezeichnet in der Kryptografie eine geheime Information (privater Schlüssel) oder ein öffentliches Gegenstück dazu (öffentlicher Schlüssel). Es gibt Verfahren, bei denen jeweils mit dem gleichen privaten Schlüssel ver- und entschlüsselt wird sowie Verfahren bei denen ein öffentlicher Schlüssel zum Verschlüsseln und ein privater zum Entschlüsseln verwendet wird.
Schlüsselkompro-mittierung	Ein privater Schlüssel (Private Key) gilt als kompromittiert, wenn sein Wert einer nicht autorisierten Person offen gelegt wurde, eine nicht autorisierten Person Zugriff auf ihn hatte oder es eine praktische Methode gibt, mit der eine nicht autorisierte Person seinen Wert ausfindig machen kann.
Secure Socket Layer (SSL)	Vorgängerbezeichnung der Transport Layer Security. Weitere Erklärungen siehe Transport Layer Security.
Signatur	Siehe digitale Signatur.
Smartcard	Chipkarte mit Rechenfunktionalität, die für kryptografische Zwecke verwendet werden kann.
Simple Object Access Protocol (SOAP)	Simple Object Access Protocol: SOAP stellt einen einfachen Mechanismus zum Austausch von strukturierter Information zwischen Anwendungen in einer dezentralisierten, verteilten Umgebung zur Verfügung.
Sperrinstanz	Komponente, die Zertifikatssperrungen durchführt.
Sperrliste	Liste, in der gesperrte digitale Zertifikate aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats sollte anhand einer

	Sperrliste überprüft werden, ob dieses noch verwendet werden darf. Wird auch als Certificate Revocation List (CRL) bezeichnet.
Stammzertifizierungs-stelle (Root-CA)	Die oberste Zertifizierungsstelle, deren Stammzertifikat von Anwendungssoftwareanbietern verteilt wird und die untergeordnete CA-Zertifikate (Sub-CA) ausstellt.
Subject Alternative Name	Zusätzliche Felder in einem Zertifikat. Die Felder müssen mindestens einen zusätzlichen Namen des Zertifikatinhabers enthalten und sind eine Standarderweiterung des X509 Standards.
Subject- Distinguished Name (Subject-DN)	Subject = engl. Subject (Person oder Maschine). Format, mit dem gemäß dem X.500- und dem LDAP-Standard eindeutige Namen angegeben werden können. Der Subject-DN bezeichnet eindeutig den Zertifikatsinhaber.
Subjekt	Die natürliche Person, das Gerät, System, die Einheit oder juristische Person, die in einem Zertifikat als Subjekt benannt wird. Das Subjekt ist entweder der Zertifikatnehmer oder ein Gerät, das der Kontrolle des Zertifikatnehmers untersteht oder von diesem betrieben wird.
Suspension	Im Zusammenhang von PKI ist unter Suspendierung die vorläufige bzw. temporäre Sperrung zu verstehen. Das Zertifikat erscheint zunächst in der Zertifikatssperrliste kann aber durch den Registrator wieder aktiv geschaltet werden.
Trust Center Advisory Board	Gremium innerhalb der DT Security GmbH das über PKI-Funktionalitäten entscheidet.
Transport Layer Security (TLS)	Krypto-Protokoll zur Absicherung von Ende-zu-Ende-Verbindungen im Internet. Kann ihn vielen Fällen statt dem komplexeren IPSec verwendet werden.
Unified Communications Certificates (UCC)	Zertifikate, die es ermöglichen, die Subject Alternative Name Felder zu verwenden. Es können somit mehrere Namen mit einem Zertifikat abgesichert werden.
Untergeordnete Zertifizierungsstelle (Sub-CA)	Eine Zertifizierungsstelle, deren Zertifikat von der Stammzertifizierungsstelle (Root-CA) oder einer anderen untergeordneten Zertifizierungsstelle (Sub-CA) signiert wird.
Validierung	Ein Nachweis der Reproduzierbarkeit eines Ergebnisses aus einer beschriebenen Vorgehensweise unter definierten Bedingungen. Je exakter eine Vorgehensweise beschrieben ist und je weniger unbekannte Einflussfaktoren bestehen, desto sicherer ist es, übereinstimmende Resultate zu erzeugen. Für eine Validierung benötigt man die Beschreibung des Zieles und des Weges. Valide bedeutet in diesem Zusammenhang, dass der Weg wiederholbar zum Ziel führt. Im Kontext einer PKI besteht ein Validierungsprozess z.B. an folgenden Stellen: ▪ Mitteilung und Prüfung einer Identität (z.B. natürliche Person, Gerät) gegenüber dem Zertifikatsantrag. ▪ Algorithmus zur Überprüfung eines Zertifikats auf Gültigkeitsdauer (Gültigkeitszeitraum), ausstellende Zertifizierungsstellen und Zertifikatsstatus (gültig, gesperrt).
Verbundenes Unter-nehmen (Affiliate)	Beispielsweise ein Unternehmen, eine Partnerschaft, ein Joint Venture, Körperschaft, (Kapital) Gesellschaft, Verband, Stiftung

	oder eine andere Organisation (juristische Person), welche eine andere Organisation (juristische Person), Einrichtung, Abteilung, Gebietskörperschaft oder eine Einheit, die einer Regierungsbehörde direkt unterstellt ist, beaufsichtigt, von dieser beaufsichtigt wird oder mit dieser einer gemeinsamen Kontrolle untersteht.
Vertrauende Dritte (Relying Parties)	Eine natürliche oder juristische Person (z.B. Firma, Organisation) die im Vertrauen auf die Funktion eines Zertifikats handelt.
Verzeichnisdienst	Datenspeicher, der den Abruf von Zertifikaten und Informationen über Zertifikate (insbesondere Sperrlisten) ermöglicht.
Voll qualifizierter Domain-Name (FQDN)	Korrekter und vollständiger Domain-Name, d.h. Verkettung aller Labels eines Pfades im Domain-Namensraum (weitere Informationen siehe RFC 2181).
Web-Request	Variante eines Zertifikatsauftrags, bei dem die Daten über ein Web-Formular an die Zertifizierungsstelle übermittelt werden.
WebTrust	Überprüfung und Bestätigung für Zertifizierungsstellen (WebTrust for Certification Authorities) durch ein unabhängiges Wirtschaftsprüfer-unternehmens das die PKI nach den WebTrust-Kriterien „American Institut of Certified Public Accountants“ (AICPA) betrieben werden. Ziel der WebTrust-Prüfungen ist es, das Vertrauen der Nachfrageseite in den elektronischen Geschäftsverkehr zu stärken.
Wildcard-Zertifikat	Ein Zertifikat, das ein Sternchen (*) in der äußersten linken Position eines in dem Zertifikat enthaltenen voll qualifizierten Domain-Namens (Fully-Qualified Domain Names) des Subjekts aufweist.
Wurzelzertifizierungsstelle	Siehe Stammzertifizierungs-stelle (Root-CA)
X.509	Standard, dessen wichtigster Bestandteil ein Format für digitale Zertifikate ist. Zertifikate der Version X.509v3 werden in allen gängigen Public-Key-Infrastrukturen unterstützt.
Zertifikat	Siehe digitales Zertifikat.
Zertifikatsnehmer	Eine natürliche oder juristische Person, der ein Zertifikat ausgestellt wird und die rechtlich durch einen Bezugsvertrag oder Nutzungsbedingungen gebunden ist.
Zertifizierungsstelle	Komponente, die digitale Zertifikate ausstellt, indem sie einen Datensatz bestehend aus öffentlichem Schlüssel, Name und verschiedenen anderen Daten digital signiert. Ebenso werden von der Zertifizierungsstelle Sperrinformationen herausgegeben.
zLint	Ein Tool, das Zertifikate hinsichtlich der Konsistenz mit RFC5280 und [CABF-BR] überprüft.
Zuverlässige öffentliche Datenquelle	Ein Authentifizierungsdokument oder eine Datenquelle (z.B. Identitätsdatenbank, Handelsregister), anhand der Subjektidentitätsdaten überprüft werden und die im Allgemeinen von kommerziellen Unternehmen und Behörde (öffentliche Verwaltung) als zuverlässig anerkannt wird und die von einer dritten Partei für einen anderen Zweck als der Zertifikatsausstellung durch den Antragsteller erstellt wurde.

12AKRONYME

Tabelle 12: Erweiterung „Akronyme“

Akronym	Erklärung
AGB	Allgemeine Geschäftsbedingungen
AICPA	American Institute of Certified Public Accountants
ASP	Application Service Provider
ARL	Authority Revocation List
CA	Certification Authority
CAA	Certification Authority Authorization
CP	Certificate Policy
CPS	Certification Practice Statement
CN	Common Name
CRL	Certificate Revocation List
CT	Certificate Transparency
DCF77	Zeitzeichensender (Langwellensender) in Mainflingen bei Frankfurt am Main
DIN	Deutsches Institut für Normung eV
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name Systems
DTAG	Deutsche Telekom AG
eIDAS	Verordnung über elektronische Identifizierung und Vertrauensdienste (electronic Identification and Signature)
ETSI	Das Europäische Institut für Telekommunikationsnormen, engl. ETSI (European Telecommunications Standards Institute). ETSI ist eine gemeinnützige Organisation, welche offiziell von der Europäischen Union als Europäische Organisation für Normung anerkannt ist und das Ziel verfolgt, weltweit anwendbare Standards für die Informations- und Kommunikationstechnologien zu schaffen.
EV	Extended Validation
EVCP	“Extended Validation” Certificate Policy
FQDN	Fully Qualified Domain Name
GPS	Global Positioning System
GR	Kennzeichner für Gruppen, Funktions-, Rollenzertifikat
HSM	Hardware Security Modul
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force

IPSec	Internet Protocol Security
ISMS	Information Security Management System (Managementsystem für Informationssicherheit)
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVCP	“Organizational Validation” Certificate Policy
PIN	Personal Identification Number
PKI	Public Key Infrastruktur
PKIX	Public Key Infrastructure X.509
PN	Kennzeichner für Pseudonym
PSE	Personal Security Environment
PU	Productive Unit (Wirkumgebung)
RA	Registration Authority
RAOP	RA Operator (Auftragsbearbeitung / Validierungsexperte / Validierungsspezialist)
RFC	Requests for Comments
RSA	Rivest Shamir Adleman
SCT	Signed Certificate Timestamp
S/MIME	Secure Multipurpose Internet Mail Extension
SAN	Siehe Subject Alternative Name
SigG	Signaturgesetz
SigV	Signaturverordnung
SOAP	Simple Object Access Protocol
SOGIS	Senior Officials Group Information Systems Security
SSL	Secure Socket Layer
TLS	Transport Layer Security
TU	Test Unit (Test-Umgebung)
UCC	Unified Communications Certificates.
UPN	User Principal Name
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
XML	Extensible Markup Language