Tabelle Änderungshistorie

Version	Stand	Bearbeiter	Änderung / Kommentar
1.00	Stand 01.09.2023	Christoph Luxem	Initiale Version des CPS nach RFC 3637

Inhaltsverzeichnis

1 Einleitung

1.1 Überblick

Dieses Dokument fasst die verbindlichen Zertifizierungsrichtlinien der Public Key Infrastructure (im folgenden PKI) für die Ausstellung von Zertifikaten zur Verschlüsselung und Authentisierung in einem Certification Practice Statement (CPS) zusammen. Die oberste Zertifizierungsstelle wird als PCA (Policy Certification Authority) bezeichnet. Im folgenden Dokument wird Policy Certification Authority mit PCA abgekürzt.

Die von den Spitzenverbänden der gesetzlichen Krankenkassen eingerichtete

- Informationstechnische Servicestelle der gesetzlichen Krankenkassen GmbH (ITSG)
- die von der Deutschen Krankenhausgesellschaft eingerichtete
  Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH (DKTIG) und die
- Datenstelle der Rentenversicherung (DSRV),
  unterhalten von der „Deutschen Rentenversicherung Bund“

haben sich auf eine gemeinsame Gestaltung der PCA-Datenübermittlung im Gesundheits- und Sozialwesen verständigt. Die o.g. Organisationen betreiben die PCA als gleichberechtigte Partner zur Verbesserung der Sicherheit des Datenaustausches (Anlage 16; Abschnitt 1.1.).

„*Primäres Ziel ist die Sicherheit der Kommunikation im Rahmen des Datenaustausches zwischen der GKV, GRV und anderen Leistungserbringern, die über eine IK -Nummer, sowie Arbeitgebern / Zahlstellen, die über eine Betriebsnummer oder Zahlstellennummer verfügen*“ (siehe Anlage 16; Abschnitt 5.3.2).

Die „Policy Certification Authority“ (PCA) kann von Teilnehmern aus dem Gesundheits– und Sozialwesen in Anspruch genommen werden. Daneben können nicht nur Certificate Authorities aus dem Gesundheitswesen oder dem Bereich der Rentenversicherung, sondern darüber hinaus können ggf. auch CA‘s und Teilnehmer aus anderen Bereichen des Sozialwesens die Funktion der PCA in Anspruch nehmen (siehe Anlage 16; Abschnitt 5.3.2).“

Die technischen Anforderungen für die Certification Authority sind in „Gemeinsame Grundsätze Technik“ des Gesetzlichen Krankenkassen Verband (GKV) festgelegt. Es wird hier insbesondere für die technischen Anforderungen auf die Anlage 16 zur Security Schnittstelle (SECON) verwiesen „https://www.gkv-datenaustausch.de/technische_standards_1/technische_standards.jsp“.

1.2 Die Gliederung des Dokumentes erfolgt nach dem RFC 3647

Name:	PCA Certificate Policy (CPS)
Version:	1.0.0
Datum:	22.12.2024
OID:	X.X.X.X.X.X.XXXX.XXX.X.X

1.3 PKI-Teilnehmer / Beteiligten

1.3.1 Zertifizierungsstellen

Für die PKI wird eine zweistufige Zertifizierungsstruktur mit einem selbstsignierten PCA-Root-Zertifikat verwendet. Das PCA zertifiziert ausschließlich nachgelagerte fachliche CAs für die Nutzung als Zertifizierungszertifikate für Zertifizierungsstellen.

Die der PCA nachgelagerten fachlichen Zertifizierungsstellen und Verfahren sind:

- die Zertifizierungsstelle für das Leistungserbringerverfahren (DALE),
- die Zertifizierungsstelle für das Arbeitgeberverfahren (AGV) und
- die Zertifizierungsstelle für das Verfahren der Datenübertragung gem. § 301 SGB V für den Zugang der Krankenhäuser sowie Vorsorge- und Rehabilitationseinrichtungen der Telematik.

Die nachgenannten fachlichen Zertifizierungsstellen erstellen Endnutzerzertifikate (End-Entity-Zertifikate) für die sichere Kommunikation im Gesundheits- und Sozialwesen.

Kontaktdaten: DKTIG GmbH

Humboldstr.9
04105 Leipzig
E-Mail: trustcenter@dktig.de
Telefon: +49 341308951-0

Kontaktformular: https://dktig.de/kontakt/

Homepage: www.dktig.de

Kontaktdaten: ITSG GmbH

ITSG GmbH - Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH
Seligenstädter Grund 11
63150 Heusenstamm

Kontaktformular: https://www.itsg.de/kontakt-trust-center/
Telefon: +49 06104/60050-0

1.3.2 Registrierungsstellen (RA)

Die Registrierungsstellen überprüfen die Identität und Authentizität von Antragsstellern und Auftraggebern gemäß den „Gemeinsame Grundsätze Technik“ des Gesetzlichen Krankenkassen Verband (GKV) in der Anlage 16 zur Security Schnittstelle (SECON).

Das Erfordernis der Prüfung der Identität und Authentizität ist an jeder Stelle der Vertrauenskette zu gewährleisten und umfasst die Erneuerung bestehender PCA und Sub-CA Zertifikate wie auch gegebenenfalls Anträge für neue CAs, Verfahren und neue Zertifizierungsstellen. Zum Registrierungsverfahren siehe auch im Abschnitt 3.2 in diesem Dokument.

1.3.3 Zertifikatsnehmer und Zertifikatsnutzer

Zertifikatsnehmer der PCA sind die nachgeordneten Zertifizierungsstellen. Die Zertifizierungsstellen werden von den unter Abschnitt 1.1 genannten Auftraggebern betrieben.

Hierbei handelt es sich um die von den gesetzlichen Krankenkassen eingerichtete:

- Informationstechnische Servicestelle der Gesetzlichen Krankenkassen GmbH (ITSG)
- die von der Deutschen Krankenhausgesellschaft eingerichtete
  Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH (DKTIG) und der
- Datenstelle der Rentenversicherung (DSRV)
  unterhalten von der „Deutschen Rentenversicherung Bund“.

1.3.4 Vertrauender Dritter (Relying parties)

Vertrauende Dritte (Relying parties) sind alle natürlichen Personen oder Gesellschaften, die sich auf die Vertrauenswürdigkeit des von der PKI ausgestellten Zertifikate oder Signaturen verlassen.

1.3.5 Andere Teilnehmer

Mit DV-technischen Aufgaben als technischer Dienstleister ist die Eviden Germany GmbH betraut. Im folgenden Text technischer Dienstleister genannt.

1.4 Verwendungen von Zertifikaten

1.4.1 Erlaubte Verwendung von Zertifikaten

Die folgenden Schlüsselverwendungen sind für die aufgeführten Certification Authorities (DKTIG, DALE und AGV) erlaubt:

- Zertifikatsignatur
- Offline-Signieren der Zertifikatsperrliste
- Signieren der Zertifikatsperrliste.

Die PCA (Policy Certification Authority) zertifiziert nachgelagerte fachliche CAs (Certification Authorities) für die Zertifikatsnehmer. Die der PCA nachgeordneten CAs werden für die Erstellung von Benutzerzertifikaten für eine sichere Kommunikation im Gesundheitswesen und Sozialwesen genutzt.

Für die folgenden CAs und Verfahren wird die PCA als Root-Zertifikat verwendet:

- CA: ITSG TrustCenter für Arbeitgeber (AGV)

- CA: ITSG TrustCenter für sonstige Leistungserbringer (DALE)
- CA: DKTIG TrustCenter für Krankenhäuser und Leistungserbringer PKC (DKTIG).

1.4.2 Verbotene Verwendungen

Die Nutzung ist auf die in der Policy beschriebene Verwendung (Abschnitt 1.4.1) begrenzt.
Die erstellten Zertifizierungsstellenzertifikate sind nicht zur Weitergabe vorgesehen. Eine private Verwendung der Zertifikate ist untersagt.

1.5 Verwaltung der Zertifizierungsrichtlinien

1.5.1 Zuständigkeit für das CPS-Dokument

Dieses CPS-Dokument wird von den Betreibern der PKI gepflegt.

1.5.2 Ansprechpartner und Kontakte

Die Meldungen von Missbrauch und Kompromittierung von Zertifikaten und Schlüsseln können unter der folgenden URL abgesetzt werden:

Kontaktinformationen ITSG GmbH

- Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung (ITSG)
- E-Mail: kontakt@itsg.de
- URL.: https://www.itsg.de/

Kontaktinformationen DKTIG GmbH:

- **Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH (DKTIG)**
- E-Mail: mail@dktig.de
- URL: https://dktig.de/kontakt/

1.5.3 Prüfung der Zertifizierungsrichtlinie

Das Certification Practice Statement (CPS) wird einem jährlichen Review unterzogen. Daneben erfolgt eine Überprüfung bei besonderen Anlässen. Änderungen und Review werden in der Änderungshistorie vermerkt, auch wenn keine inhaltlichen Änderungen vorgenommen werden.

Die Änderungen des CPS wird von den beteiligten Partnern (siehe Beteiligte 1.1) sowie dem Spitzenverband der gesetzlichen Krankenkassen freigegeben.

1.5.4 Veröffentlichung der Zertifikatsrichtlinien

Das CPS wird auf der Homepage der beteiligten Zertifizierungsstellen veröffentlicht.

1.6 Definitionen und Abkürzungen

(siehe Abschnitt 10 Abkürzungen)

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Die Informationen zu den öffentlichen Zertifikaten der PKI einschließlich des Root-Zertifikats der PCA stehen auf der Homepage der beteiligten Zertifizierungsstellen (CA) zur Verfügung.

Im von der PKI genutzten Whitelist-Verfahren werden täglich in Form der „Gesamtlisten“ alle gültigen Zertifikate für die Teilnehmer bereitgestellt. Die gültigen Zertifikate der unterschiedlichen Verfahren DALE, AGV und DKTIG werden über Gesamtlisten und LDIF-Dateien für LDAP-Directory den Teilnehmern der PKI werktäglich zur Verfügung gestellt.

Die Gesamtlisten sind hierarchisch unter den gültigen PCA und Sub-CA Zertifikaten aufgebaut. PCA und Sub-CA Zertifikate bleiben so lange in den Gesamtlisten, bis ihre Gültigkeit ausgelaufen ist, sie gesperrt wurden oder keine durch sie ausgestellte gültigen Zertifikate mehr existieren.

Die Benutzerzertifikate befinden sich in den Gesamtlisten nach Seriennummern sortiert unter den CA-Zertifikaten, durch die sie bei der Erstellung signiert wurden. Die Gesamtlisten können auf Homepages der Zertifizierungsstellen geladen werden.

Daneben werden auch die Sperrlisten zusammen mit den Gesamtlisten an die Teilnehmer zur Verfügung gestellt. Die PCA besitzt entsprechend der Anlage 16 keine eigene Sperrliste für die Sub-CA Zertifikate.

Für das Arbeitgeberverfahren existieren folgende Schlüssellisten mit öffentlichen Teilnehmerschlüsseln:

- gesamt-pkcs.agv (alle Teilnehmerschlüssel mit 4096 Bit Schlüssellänge)
- gesamt-rsa4096.agv (optional, alle Teilnehmerschlüssel mit 4096 Bit Schlüssellänge)
- annahme-rsa4096.agv (Schlüssel der Datenannahmestellen mit 4096 Bit Schlüssellänge)
- sperrliste-ag-rsa4096.crl (gesperrte Teilnehmerschlüssel mit 4096 Bit Schlüssellänge)

Für das Leistungserbringerverfahren existieren folgende Schlüssellisten mit öffentlichen Teilnehmerschlüsseln:

- gesamt-pkcs.key (alle Teilnehmerschlüssel mit 4096 Bit Schlüssellänge)
- gesamt-rsa4096.key (optional, alle Teilnehmerschlüssel mit 4096 Bit Schlüssellänge)
- annahme-rsa4096.key (Schlüssel der Datenannahmestellen mit 4096 Bit Schlüssellänge)
- pkv-rsa4096.key (Sonderliste mit Schlüssel der PKV mit 4096 Bit Schlüssellänge)
- sperrliste-le-rsa4096.crl (gesperrte Teilnehmerschlüssel mit 4096 Bit Schlüssellänge)

ITSG -TrustCenter

Die Informationstechnische Servicestelle der Gesetzlichen Krankenversicherungen (ITSG) stellt die Informationen zu den öffentlichen PCA-(Root) Zertifikaten auf der Homepage unter folgenden Links zur Verfügung:

- https://www.itsg.de/produkte/trust-center/
- https://www.itsg.de/produkte/trust-center/oeffentliche-zertifikate-und-verzeichnisse/
- https://www.itsg-trust.de/all/oav.php?

DKTIG -TrustCenter

Die Schlüsselverzeichnisse der Annahmestellen (§ 301 SGB V Datenübermittlung) der GKV und der PKV stehen auf der Homepage des Trustcenter der DKTIG für den Download zur Verfügung:

- https://dktig.de/downloads-zertifikate/

2.2 Veröffentlichung von Informationen zu Zertifikaten

Die ITSG GmbH veröffentlicht die folgenden Informationen:

- https://www.itsg.de/produkte/trust-center/oeffentliche-zertifikate-und-verzeichnisse/

- PCA Root Zertifikate
- Sub CA -Zertifikate für das Arbeitgeberverfahren
- Sub CA -Zertifikate für das Leistungserbringerverfahren
- Sperrlisten für das Arbeitgeberverfahren
- Sperrlisten für das Leistungserbringerverfahren
- LDIF-Dateien für die Nutzer eines LDAP-Verzeichnisses der ITSG
- Certificate Policy und Certification Practice Statement

Die DKTIG GmbH veröffentlicht die folgenden Informationen:

- https://dktig.de/downloads-zertifikate/
- Certificate Policy und Certification Practice Statement

Daneben werden auf den Seiten auch bereitgestellt:

- Beschreibungen des Antragsverfahrens
- Formulare zur Beantragung von Zertifikaten
- Informationen zum Sperrprozess

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Für die Veröffentlichung der PCA und CA-Zertifikate sowie der CP (Richtlinie) und des CPS (Zertifizierungsbetrieb) gelten die folgenden Intervalle:

PCA der Trust Center

PCA für das Arbeitgeber- und Leistungserbringerverfahren	Tag des Schlüsselwechsels

ITSG Trust Center

ITSG CA für das Leistungserbringerverfahren	Tag des Schlüsselwechsels
ITSG CA für das Arbeitgeberverfahren	Tag des Schlüsselwechsels
Certificate Policy (CP)	Anlassbedingter Aktualisierung sowie jährliche Überprüfung der CP auf Aktualität.
Certification Practice Statement (CPS)	Anlassbedingter Aktualisierung sowie jährliche Überprüfung des CPS auf Aktualität.
Sperrlisten	Anlassbedingte Aktualisierung nach Sperrungen sowie turnusmäßig Veröffentlichung am ersten Werktag der Woche
LDIF-Dateien für LDAP-Verzeichnis	LDIF-Dateien für Teilnehmer der PKI

DKTIG Trust Center

DKTIG CA für das Leistungserbringerverfahren	Tag des Schlüsselwechsels

Certificate Policy (CP)	Nach Erstellung bzw. Aktualisierung und Freigabe.
Certification Practice Statement (CPS)	Nach Erstellung bzw. Aktualisierung und Freigabe.

2.4 Zugang zu den Informationsdiensten

Die an der PKI beteiligten Nutzer bzw. Teilnehmer erhalten werktäglich die Gesamtlisten auf dem aktuellen Stand.

Auf den Webseiten der beteiligten TrustCenter werden die jeweils gültigen PCA und untergeordneten CA-Zertifikate für den öffentlichen unbeschränkten Download bereitgestellt.

2.4.1 ITSG-TrustCenter

PCA (Policy Certification Authority): Datenaustausch im Gesundheits- und Sozialwesen insb.

- CA: ITSG TrustCenter für Arbeitgeber
- CA: ITSG TrustCenter für sonstige Leistungserbringer

Wurzelzertifikat der PCA: Organisation (o): Datenaustausch im Gesundheits- und Sozialwesen

Seriennummer: (dc): 80 / (hex): 50

- Gültigkeitszeitraum: 30.11.2021 bis 30.01.2029
- Signaturhashalgorithmus: SHA256
- Signaturalgorithmus: RSASSA-PSS
- Schlüssellänge: RSA 4096 Bits
- SHA1-Fingerprint: 6476a953c92e279776875cf1b52b3a7bdfb1d874
- https-Download: (rechte Maustaste, Ziel speichern unter)

PCA-50.der (DER-Format, DER-codiert-binär X.509)
md5 Datei-Hash: cb4acf8ad779f24ef17dff049671fe1b

PCA-50.pem (PEM-Format, Base64-codiert X.509)
md5 Datei-Hash: 573624e7906f204512cd9fc691447456

Untergeordnete CA: Organisation (o): ITSG TrustCenter für Arbeitgeber

- Seriennummer (dc): 82 / (hex): 52
- Gültigkeitszeitraum: 30.11.2021 bis 06.01.2027
- Signaturhashalgorithmus: SHA256
- Signaturalgorithmus: RSASSA-PSS
- Schlüssellänge: RSA 4096 Bits
- SHA1-Fingerprint: 2757c66d1897f6912e7a5d962c147d552c10a6d3

CA-52.der (DER-Format, DER-codiert-binär X.509)
md5 Datei-Hash: 9fe506e043211e299954c9f830c83ae2

CA-52.pem (PEM-Format, Base64-codiert X.509)
md5 Datei-Hash: 1079d06971945f5952c5263d102c435b

Untergeordnete CA: Organisation (o): ITSG TrustCenter für sonstige Leistungserbringer

(1) ZERTIFIKATE MIT RSASSA-PSS-SIGNATURALGORITHMUS

- Seriennummer (dc):81/ (hex): 51
- Gültigkeitszeitraum: 30.11.2021 bis 06.01.2027
- Signaturhashalgorithmus: SHA256
- Signaturalgorithmus: RSASSA-PSS
- Schlüssellänge: RSA 4096 Bits
- SHA1-Fingerprint: 9539ec92972f6795502b41183d027f7ec3ba5e49

CA-51.der (DER-Format, DER-codiert-binär X.509)
md5 Datei-Hash: 0d231df52fbc845f688145d938d9f718

CA-51.pem (PEM-Format, Base64-codiert X.509)
md5 Datei-Hash: ebc9d8017f2a0eb609978d650ddad628

(2) ZERTIFIKATE MIT RSASSA-PSS-SIGNATURALGORITHMUS

- Seriennummer (dc): 84 / (hex): 54
- Gültigkeitszeitraum: 28.11.2023 bis 07.01.2029
- Signaturhashalgorithmus: SHA256
- Signaturalgorithmus: RSASSA-PSS
- Schlüssellänge: RSA 4096 Bits
- SHA1-Fingerprint: 1298f7e78a42133c52b6b4c01d0ee1703f75d6cb

- CA-54.der(DER-Format, DER-codiert-binär X.509)
  md5 Datei-Hash: bb9a9659e3eca801956acca345929738
- CA-54.pem (PEM-Format, Base64-codiert X.509)
  md5 Datei-Hash: c8f7eacf15a653db0132e84ca8103653

2.4.2 DKTIG-TrustCenter

PCA (Policy Certification Authority): Datenaustausch im Gesundheits- und Sozialwesen ist das Wurzelzertifikat für den Datenaustausch im Gesundheits- und Sozialwesen

- Seriennummer (dc): 80 / (hex): 50
- Gültigkeitszeitraum 30.November 2021 / 30. Januar 2029
- Signaturhashalgorithmus: SHA256
- Signaturalgorithmus: rsassaPss
- Schlüssellänge: RSA 4096 Bits
- Sha1-Fingerprint: 6476a953c92e279776875cf1b52b3a7bdfb1d874

PCA-50.der (DER-Format, DER-codiert-binär X.509)
md5 Datei-Hash: cb4acf8ad779f24ef17dff049671fe1b

PCA-50.pem (PEM-Format, Base64-codiert X.509)
md5 Datei-Hash: 573624e7906f204512cd9fc691447456

Untergeordnete CA: Organisation(o): DKTIG TrustCenter fuer Krankenhaeuser und Leistungserbringer (PKC): Verfahren nach § 301 SGB V.

(1) ZERTIFIKATE MIT RSASSA-PSS-SIGNATURALGORITHMUS

- Seriennummer (dc): 83 / (hex): 53
- Gültigkeitszeitraum 30.November 2021 / 05. Januar 2027
- Signaturhashalgorithmus: SHA256
- Signaturalgorithmus: rsassaPss
- Schlüssellänge: RSA 4096 Bits
- SHA1-Fingerprint: a5a2b31b724599f999a68220a6caf58f67bae5bd

Download: Zertifikate der DKTIG https://dktig.de/downloads-zertifikate/

Öffentliche Schlüsselverzeichnisse für Arbeitgeber und Leistungserbringerverfahren:

https://www.itsg.de/produkte/trust-center/oeffentliche-zertifikate-und-verzeichnisse/

(2) ZERTIFIKATE MIT RSASSA-PSS-SIGNATURALGORITHMUS

- Seriennummer (dc): 84 / (hex): 54
- Gültigkeitszeitraum: 28.11.2023 bis 07.01.2029
- Signaturhashalgorithmus: SHA256
- Signaturalgorithmus: rsassaPss
- Schlüssellänge: RSA 4096 Bits
- Sha1-Fingerprint: e659f9b9878872c25fa3e5c31e08cba86c54e9a2

- CA-54.der (DER-Format, DER-codiert-binär X.509)
  md5 Datei-Hash: bb9a9659e3eca801956acca345929738

- CA-54.pem (PEM-Format, Base64-codiert X.509)
  md5 Datei-Hash: c8f7eacf15a653db0132e84ca8103653

3 Identifizierung und Authentifizierung

3.1 Namen

Der Name der ausgestellten Zertifikate (Distinguished Name = DN) richtet sich nach dem Standard x500. Über den Distinguished Name ist eine eindeutige Unterscheidung gegeben. Der DN stellt daher sicher, dass keine digitalen Zertifikate für unterschiedliche Personen mit dem gleichen Namen ausgestellt werden.

3.1.1. Namensform

Das Datenfeld „Issuer“ gibt den eindeutigen Namen des Zertifikatserzeugers (der CA) an. Mit dem Distinguished Name ist eine weltweite eindeutige Unterscheidbarkeit von Personen und Systemen gegeben. Folgende Felder sind nach dem x.500 – Standard definiert.

Aufbau des DNs für Zertifizierungsstellen (PCA) (s. Anlage 16, Abschnitt 4.4.4.u. 4.4.5.):

Pos.	Attribute		Erläuterung
1	CountryName (verpflichtend)	C	Zweistelliges Kürzel für die Länderkennung, wie “DE” für Deutschland.
2	OrganizationName (verpflichtend, fest)	O	Name der PCA als feste Zeichenkette: „Datenaustausch im Gesundheits- und Sozialwesen“

Aufbau des DN für nachgeordneten Zertifizierungsstellen (s. Sub-CA, Anlage 16, Abschnitt 4.4.5):

Pos.	Attribute		Erläuterung
1	CountryName (verpflichtend)	C	Zweistelliges Kürzel für die Länderkennung, wie „DE“ für Deutschland.
2	OrganizationName (verpflichtend)	O	Name des TrustCenters als Zeichenkette. - „ITSG TrustCenter fuer Arbeitgeber“ - „ITSG TrustCenter fuer sonstige Leistungserbringer“. - „DKTIG TrustCenter fuer Krankenhaeuser und Leistungserbringer (PKC)“

3.1.2 Aussagekraft der Namen

Das Datenfeld „issuer“ für die PCA enthält den Namen:

„Datenaustausch im Gesundheits- und Sozialwesen“.

Das Datenfeld „issuer“ für die CA gibt den eindeutigen Namen des Zertifikaterzeugers an.

3.1.3 Anonymität oder Pseudonyme

Anonymisierungen im Namen von Zertifikaten sind nicht erlaubt.

3.1.4 Regeln zur Interpretation verschiedener Namenformen

(Nichtzutreffend). Weitere Parameter sind derzeit nicht für den Namen relevant.

3.1.5. Eindeutigkeit von Namen

Der Namen muss eindeutig sein, um eine Feststellung des Zertifikatsinhabers ohne Verwechslungsgefahr zu ermöglichen. Die PCA und Sub-CA Zertifikate werden u.a. über Seriennummer (hexadezimal und dezimal) unterschieden.

3.1.6 Anerkennung, Authentifizierung und Funktion von Warenzeichen und Markennamen

Der Antragsteller und der Zertifikatsnehmer sind für die Überprüfungen verantwortlich.

3.2 Identitätsüberprüfung bei Neuantrag

Die Regelungen für die Identitätsprüfung werden entsprechend auf andere Anträge angewendet. Die Anwendung der Regeln über die Identitätsprüfung gelten grundsätzlich auch für die Beteiligung an der Erstellung der PCA als Root-CA und für die Sub-CA Zertifikate.

3.2.1 Nachweis des Besitzes des privaten Schlüssels

Der für die Erstellung des Zertifikats mit dem Antrag gesendete PKCS#10-Request muss durch dazugehörigen privaten Schlüssel des Antragstellers signiert werden, um den Besitz des privaten Schlüssels nachzuweisen.

Bei der Neuerstellung der PCA und der Sub-CA -Zertifikate werden die neuen Schlüsselpaare während der Zeremonie vor Ort im abgesicherten Bereich in einem Hardware Security Module (HSM) erstellt.

3.2.2 Authentifizierung einer Organisation

Authentifiziert werden die Ansprechpartner für das Zertifikat. Die Authentifizierung einer Organisation durch das TrustCenter ist direkt nicht vorgesehen.

3.2.3 Authentifizierung natürlicher Personen

Die Vertrauenskette muss auf allen Stufen auch bei der PCA und Zertifizierungsstellen eingehalten werden. Bei der Authentifizierung und Identifizierung natürliche Personen für die Auftraggeber und Sub-CA werden gegebenenfalls Verfahren zur Prüfung der Identität herangezogen.

Zu den Verfahren gehören u.a.:

- Personalausweis mit eID-Funktion
- Postidentifikationsverfahren.

3.2.4 Nicht überprüfte Zertifikatsnehmer Informationen

Die ausgestellten Root – und Sub-CA Zertifikate beinhalten keine ungeprüften Subjekt-Informationen.

3.2.5 Prüfung der Berechtigung zur Antragsstellung

Die Autorisierung einer natürlichen Person erfolgt als Handlungsberechtigter im Namen einer Organisation nach einem dafür geeigneten und vorgesehen Verfahren (siehe Abschnitt 3.2.3 in der vorliegenden CPS).

3.2.6 Kriterien für Cross-Zertifizierung und Interoperabilität

Eine Cross-Zertifizierung ist nicht geplant.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Die Zertifikatsnehmer für PCA und Certificate Authorities werden vor Ablauf der Gültigkeit des Zertifikats erinnert und eine zeitliche und inhaltliche Planung im Hinblick auf die Aktualisierung und Erweisung der PCA und der untergeordneten CA-Zertifikate abgestimmt.

Zur Zertifikatserneuerung einer untergeordneten Zertifizierungsstelle (Sub-CA) müssen grundsätzlich die Identitätsprüfungen entsprechend zu der Erstbeauftragung durchlaufen werden. Dies gilt insbesondere bei unbekannten oder neuen Mitarbeitern. Abschnitt 3.2.3 und 3.2.5 des vorliegendes CPS werden angewendet.

3.3.2 Zertifikatserneuerung nach einer Sperrung oder Suspendierung der Zertifikate

Die Schlüsselerneuerung eines gesperrten Zertifikates ist nicht möglich. Nach der Sperrung eines Zertifikates muss ein Neuantrag erfolgen.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Nur autorisierte Personen und Institutionen können die Sperrung eines Zertifizierungsstellenzertifikates veranlassen.

Die Authentisierung für den Antrag zur Durchführung der Sperrung eines Zertifizierungsstellenzertifikates hat in einer geeigneten Art und Weise zu erfolgen (siehe Abschnitt 3.2.3.). Es ist ein unterschriebener Sperrantrag für die Durchführung der Sperrung zu stellen. Die Unterschrift des autorisierten Ansprechpartners kann durch die seines Vorgesetzten ersetzt werden.

4. Ablauforganisation (Betriebliche Anforderungen im Lebenszyklus von Zertifikaten)

4.1 Zertifikatsantrag

4.1.1 Antragsteller für ein neues Zertifizierungsstellenzertifikat

Der Zertifikatsbeauftragungsprozess für Root und Sub-CA Zertifikate findet bei einer Erstbeauftragung entsprechend den Voraussetzungen für einen Erstantrag statt. Für die Zertifizierungsstellenzertifikate sind die Zertifikatsnehmer nach Abschnitt 1.3.1 antragsberechtigt. Im Rahmen einer routinemäßigen Zertifikatserneuerung für PCA- und Sub-CA – Zertifikate bei Ablauf der Nutzungszeit der Zertifikate kann auf einen ausdrücklichen Antrag verzichtet werden, sofern eine Einigkeit über den Inhalt der neuen Zertifikate besteht.

4.1.2 Registrierungsprozess und Zuständigkeit

Die Beantragung von Zertifikaten erfolgt im Rahmen eines mehrstufigen Registrierungsprozesses.

Es werden folgende Prüfungen vorgenommen:

- Berechtigung des Antragstellers
- Vollständigkeit und Korrektheit des Antrags
- Eindeutigkeit des DN
- Prüfung der Authentizität von Personen und Organisationen (siehe auch Abschnitt 3.3.1).

Die Spitzenverbände der gesetzlichen Krankenkassen sehen gegebenenfalls eigene Prozesse und Prüfungen für neue Teilnehmer insb. neue Zertifizierungsstellen vor.

4.1.3 Zertifikatsantrag für PCA und Sub-CA

Der Zertifikatsantrag nach PKCS#10 für PCA und Sub-CA besteht aus:

- einem Distingushed Name (DN)

- einem öffentlichen Schlüssel und
- einem Satz an Erweiterungen (Extension), welche zusammen mit dem Antragsteller (mit seinem zum öffentlichen Schlüssel gehörenden privaten Schlüssel) signiert werden.

Die Schlüssel für Root CA und Sub-CA werden im Rahmen einer Schlüsselzeremonie und Vier-Augen-Prinzip in einer gesicherten Umgebung erstellt. Die Schlüsselzeremonie wird entsprechend den Rollenkonzepten von Key-Manager durchgeführt.

4.2 Bearbeitung von Zertifikatsanträgen

4.2.1 Durchführung der Identifikation und Authentifizierung

Die Identifikation und Authentifizierung von Zertifikatsnehmern werden gemäß Kapitel 3.2 (Identitätsprüfung bei Neuantrag) durchgeführt. Der Antragsteller muss die Antragsinformationen zur Verfügung stellen, die für eine Zertifikatserstellung benötigt werden und in dem vorliegenden CPS (siehe 4.1.3) aufgeführt werden. Eine Authentifizierung ist auf allen Ebenen der PKI notwendig.

4.2.2 Annahme und Ablehnung von Zertifikatsanträgen

(Nichtzutreffend)

4.2.3 Bearbeitungsdauer von Zertifikatsanträgen

(Nichtzugreffend)

4.3 Ausstellung von Zertifikaten

4.3.1 Tätigkeiten während der Ausstellung von Zertifikaten

Nach der Bearbeitung des Zertifikatsantrags werden die PCA und SubCA Schlüsselpaare im Sicherheitsbereich des Trust Centers im Vier-Augen-Prinzip erstellt und die neuen Zertifikate erzeugt.

Die Ausstellung der Root- und Sub-CA Zertifikaten unterliegt vorher festgelegten Abläufen (key ceremony) und wird protokolliert.

Das Schlüsselpaar wird im Sicherheitsbereich entsprechend den Anforderungen aus den Zertifikatsanträgen im Vier-Augen-Prinzip durch die Key-Manager erstellt.

Nach Prüfung der neu erstellten Schlüssel wird anschließend das Zertifikat erstellt. Hinsichtlich der technischen Anforderungen wird für das Zertifikat auf die Anlage 16 des GKV verwiesen, in der die Parameter (u.a. Schlüssellänge, verwendeter Signaturalgorithmus und Extension) festlegt werden.

4.3.2 Benachrichtigung des Zertifikatsauftraggeber über die Erstellung von Zertifikaten

Die Antragsteller werden über die Erstellung des Zertifikats benachrichtigt und die Zertifikate zur Prüfung und Freigabe an die Partner bzw. Auftraggeber übergeben.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme des Zertifikats

Die Annahme des Zertifikates erfolgt nach der Prüfung und Freigabe. Im Fall von Zertifikaten einer PCA oder einer untergeordneten Sub-CA soll eine ausdrückliche Erklärung der Annahme durch den Auftraggeber erfolgen.

Die Annahmebestätigung durch den Auftraggeber soll innerhalb einer bestimmten Frist erfolgen.

4.4.2 Veröffentlichung des Zertifikates durch die CA

Die PCA und die untergeordneten CA-Zertifikate werden über öffentliche Schlüsselverzeichnisse veröffentlicht. Die Zertifikate werden ebenfalls bei Neuerstellung auf den Seiten der beteiligten Zertifizierungsstellen für den Download veröffentlicht. Eine Veröffentlichung der Zertifikate im Verzeichnisdienst erfolgt mittels LDIF-Datei oder Gesamtlisten für die Teilnehmer der PKI (siehe hierzu bereits Abschnitt 2.4 „Zugang zu Informationsdiensten“).

4.4.3 Benachrichtigung weiter Instanzen durch die CA

(Nichtzutreffend)

4.5 Verwendung des Schlüsselpaars und des Zertifikats

PCA und Sub-CA Zertifikate, die auf Basis der vorliegenden CPS erstellt werden, dürfen ausschließlich für die Nutzung in Zertifizierungsstellen ausgestellt werden (siehe Abschnitt 1.4 Verwendung von Zertifikaten).

4.5.1 Die Nutzung des privaten Schlüssels und der Zertifikate erfolgt ausschließlich durch den Zertifikatsnehmer der Zertifizierungsstelle:

- Die CA legt Regelungen für die Sicherheit, Speicherung und Nutzung der privaten Schlüssel und der erstellten Zertifikate fest.
- Es müssen Beschränkungen im Hinblick auf die Verwendung der privaten Schlüssel festgelegt werden (siehe Abschnitt 1.4.1).
- Die Sperrung der Zertifikate muss unverzüglich bei einer Kompromittierung seines privaten Schlüssels durch die Zertifizierungsstelle veranlasst werden.

4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (Certificate Renewal)

Die Zertifikatserneuerung auf Basis eines bereits genutzten Schlüsselpaares ist für die Erstellung eines neuen Zertifikates nicht zulässig. Für eine Zertifikatserneuerung muss immer auch ein neues Schlüsselpaar im HSM (Hardware Security Module) erzeugt werden.

4.6.1 Bedingungen für eine Zertifikatserneuerung

(Nichtzutreffend)

4.6.2 Beauftragung einer Zertifikatserneuerung

(Nichtzutreffend)

4.6.3 Zertifikatserneuerung

(Nichtzutreffend)

4.6.4 Benachrichtigung des Zertifikatsauftraggeber
(Nichtzutreffend)

4.6.5 Annahme
Es gelten die Regelungen gemäß Abschnitt 4.4 zur Zertifikatsakzeptanz.

4.6.6 Veröffentlichung
Es gelten die Regelungen zur Veröffentlichung gemäß Abschnitt 4.4.2.

4.6.7 Benachrichtigungen weiterer Instanzen über eine *Zertifikatserneuerung* durch die CA.
(Nichtzutreffend)

4.7 Zertifikatserneuerung mit Schlüsselwechsel (Re-Keying)
Bei der Zertifikatserneuerung wird immer ein neues Paar Schlüssel generiert. Es erfolgt im Rahmen dieses Vorgangs eine Überprüfung der Aktualität der genutzten Schlüsseldaten und gegebenenfalls eine Anpassung der Schlüsseldaten.

4.8 Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung
Eine Zertifikatserneuerung wird in der Regel mit Schlüsselwechsel und einer Überprüfung der technischen Parameter durchgeführt. Die Zertifikatsinhalte und die verwendeten technische Parameter werden überprüft und aktualisiert. Die privaten Schlüssel werden gewechselt und nicht wiederverwendet.

4.8.1 Gründe für eine Zertifikatserneuerung mit Schlüsselwechsel und Anpassung von Daten und technischen Parametern
Die notwendigen Änderungen führen zu einer Zertifikatserneuerung mit Schlüsselwechsel und Anpassung der Schlüssel- und Zertifikatsparameter. Der Termin wird unter den Beteiligten (Abschnitt 1.1.) abgestimmt. Auf ein formelles Verfahren kann verzichtet werden.

Eine Zertifikatserneuerung ist notwendig bei:

- Ablauf der Nutzungszeit der CA
- Ablauf der Gültigkeit des Zertifikats
- Neubeantragung nach einer Sperrung des letzten Zertifikates
- Änderung in den Daten des bisherigen Zertifikates
- Änderungen bzw. Aktualisierungen von technischen Parametern wie Algorithmen, Schlüssellänge, Signaturalgorithmen, der Gültigkeitsdauer des Zertifikats erfolgen, wenn keine ausreichend Sicherheit der derzeitigen Zertifikate gewährleistet ist.

4.8.2 Planung und Beantragung eines Schlüsselwechsels
Der turnusmäßig vorgesehene Schlüsselwechsel ergibt sich aus den Festlegungen der Laufzeit der PCA und den untergeordneten Zertifizierungsstellenzertifikaten sowie deren Nutzungs- und Gültigkeitsdauern.

Daneben kann die außerplanmäßige Zertifikatserneuerung von den Zertifikatsnehmern und Zertifikatsauftraggeber beantragt werden.

Ist eine Erneuerung der Zertifikate aus technischen oder sicherheitstechnischen Gründen notwendig, wird die Zertifikatserneuerung zum nächsten möglichen Zeitpunkt geplant. Die Zertifikatsnehmer werden über die notwendige außerplanmäßige Zertifikatserneuerung über Webseiten informiert.

4.8.3 Ablauf der Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Der Prozess der Zertifikatserneuerung entspricht dem Verfahren der erstmaligen Zertifikatserstellung. Die Erneuerung des Schlüsselpaar sowie die Erzeugung des Zertifikats wird in einem Sicherheitsbereich durchgeführt. Der Anpassung des Zertifikats liegen in der Regel aktualisierte Anforderungen der Anlage 16 zu Grunde.

4.8.4 Benachrichtigung des Zertifikatsnehmer

Angewendet werden die initialen Regelungen für die Zertifikatserstellung. Insbesondere werden auch die Anforderungen an einen sicheren Datenaustausch mit Zertifikatsnehmer eingehalten.

4.8.5 Annahme der Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Es wird verwiesen auf die initialen Regelungen zur Ablauforganisation für die Zertifikatserstellung siehe Abschnitt 4, „Ablauforganisation“.
Die Nutzung oder Bestätigung des Empfangs reichen für die Annahme eines Zertifikats durch den Zertifikatsnehmer.

4.8.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle

Es wird verwiesen auf die initialen Regelungen für die Zertifikatserstellung (siehe Abschnitte 4.4, 4.6). Die neuen Zertifikate werden veröffentlicht auf der Webseite zum Download und mit den täglichen bereitgestellten aktuellen Gesamtlisten.

4.8.7 Benachrichtigung weiterer Instanzen über die Zertifikatserstellung

(Nichtzutreffend)

4.9 Sperrung von Zertifikaten

Die Voraussetzung, Gründe und der Ablauf der Sperrung von Sub-CA Zertifikaten durch die Root-CA müssen beschrieben werden.

4.9.1 Gründe für die Sperrung

Die PCA muss ein Sub-CA Zertifikat sperren, wenn nachfolgende Gründe vorliegen:

- Die Sub-CA stellt schriftlich einen Sperrauftrag.
- Der ursprüngliche Zertifikatsrequest war nicht autorisiert und wurde auch nicht rückwirkend autorisiert.
- Der PCA liegen Beweise vor, dass der private Schlüssel der Sub-CA kompromittiert wurde.
- Der PCA liegen Beweise vor, dass das Zertifikat missbräuchlich eingesetzt wurde.
- Die PCA erhält Kenntnis davon, dass das Zertifikat nicht entsprechend den anzuwendenden CP und CPS erstellt wurde bzw. die oder die Sub-CA nicht entsprechen der im CPS niedergeschriebenen Regelungen arbeitet.
- Die PCA entscheidet, dass Informationen im Zertifikat nicht korrekt oder missverständlich sind.
- Die PCA oder die Sub-CA stellen den Betrieb ein und haben keine Regelungen getroffen, dass im Falle einer Betriebseinstellung der Sperrsupport durch eine andere CA weitergeführt wird.
- Die PCA hat den Verdacht, dass der eigene private Schlüssel kompromittiert wurde.
- Richterliche Urteile oder die Weisung einer die Aufsicht führenden Behörde liegt vor.

4.9.2 Berechtigung eine Sperrung zu beantragen

Die Betreiber der PKI nach den Abschnitte 1.1 der CP, CPS und der Anlage 16, die untergeordneten Zertifizierungsstellen und die Spitzenverbände der gesetzlichen Krankenkassen können eine Sperrung beantragen.

4.9.3 Ablauf einer Sperrung

Die Sperrung eines Sub-Zertifikates muss schriftlich beantragt werden.

Die PCA muss Sperrungsmöglichkeiten, für die in Abschnitt 4.9.2 genannten Beteiligten bereitstellen und auf Problemreports reagieren.

4.9.4 Fristen für den Zertifikatsnehmer und Auftraggeber

Beim Vorliegen eines Sperrgrundes (Abschnitt 4.9.1) muss unverzüglich die Sperrung des Zertifikates veranlasst werden. Eine Bewertung nach 4.9.5 findet vorher statt.

4.9.5 Bearbeitungsfristen für die Zertifikatsstelle

Innerhalb von einem Tag (24h) nach Eingang einer Problemmeldung ist eine erste Analyse des Sachverhalts und ein erstes Ergebnis zu erstellen sowie dem Zertifikatsnehmer und dem Melder des Problems eine Rückmeldung zu geben.

Mit den Beteiligten (Melder und Zertifikatsnehmer) sind die Ergebnisse der Bewertung zu besprechen und gegebenenfalls zu entscheiden, ob eine Zertifikatssperrung notwendig ist.

Einfluss auf die Bewertung und Entscheidung über eine Sperrung haben insbesondere:

1. Risiko und möglicher Schaden
2. Auswirkungen der Sperrung
3. Anzahl von Meldungen zu diesem Problem
4. Behördenmeldung bzw. Strafverfolgungsbehörde.

Im Zug der Sperrung muss die sperrende CA einen entsprechenden Bericht erstellen und an Spitzenverbände und Beteiligten (nach Abschnitt 1.1 CP, CPS und Anlage 16, Abschnitt 1.1.) übermitteln.

4.9.6 Sperrprüfungen durch Zertifikatsnutzer und Relying Parties

Die PKI stellt über die werktägliche Erzeugung und Verteilung von Gesamtlisten im Rahmen einer Veröffentlichung sicher, dass die gültigen Zertifikate in Format der Gesamtlisten für die PKI nutzenden Teilnehmer bereitstehen. Die PKI beruht auf einem Whitelist-Verfahren. Die werktäglich erstellten Gesamtlisten enthalten alle gültigen PCA-, Sub-CA- und Benutzerzertifikate. Die nach der Sperrung erstellten neuen Gesamtlisten enthalten nur die gültigen Zertifikate. Wenn eine Sub-CA gesperrt wurde und diese vor der Sperrung noch gültige End-Entity Zertifikate besaß, werden diese Zertifikate in der neuen Lieferung entsprechend dem Whitelist-Verfahren bereits aus technischen Gründen nicht mehr bereitgestellt.

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Die Sperrlisten werden werktäglich neu erzeugt. Eine Sperrliste der PCA für Sub-CA Zertifikate wird nicht bereitgestellt. Die Anlage 16 sieht derzeit keine Sperrliste für Sub-CA Zertifikate vor.

4.9.8 Maximale Latenzzeit für Sperrlisten

Sperrlisten werden werktäglich zusammen mit den Gesamtlisten für die Teilnehmer der PKI bereitgestellt und übermittelt.

4.9.9 Onlinesperrung und Statusprüfung von Zertifikaten

Online-Sperrungen und Statusprüfungen stehen nicht zur Verfügung. Die Zertifikatsnutzer erhalten nach Sperrungen mit den werktäglich neu erstellten Gesamtlisten nur gültige Zertifikate. Gesperrte Zertifikate sind in Sperrlisten für End-Entity Zertifikate zu finden, die ebenfalls erstellt und mit den Gesamtlisten bereitgestellt werden.

4.9.10 Anforderungen an Online Sperr- und Statusüberprüfungsverfahren

(Nichtzutreffend)

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

(Nichtzutreffend)

4.9.12 Kompromittierung von privaten Schlüsseln

Bei der Kompromittierung des privaten Schlüssels einer PCA oder Sub-CA werden neben dem betroffenen PCA und CA-Zertifikat auch alle von ihren ausgestellten Zertifikaten gesperrt.

4.9.13 Gründe für eine Suspendierung

Für PCA und Sub-CA ist keine Suspendierung vorgesehen.

4.9.14 Beantragung einer Suspendierung

Für PCA und Sub-CA ist keine Suspendierung vorgesehen.

4.9.15 Ablauf einer Suspendierung

(Nichtzutreffend)

4.9.16 Dauer einer Suspendierung

(Nichtzutreffend)

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

Onlinesperrung und Statusprüfung für Zertifikate stehen derzeit nicht zur Verfügung. Die PKI basiert auf dem Whitelist-Verfahren.

Die gültigen PCA und CA werden über die Gesamtlisten und LDIF–Dateien werktäglich Teilnehmern zur Verfügung gestellt.

4.10.1 Betriebliche Vorgaben

(Nichtzutreffend)

4.10.2 Verfügbarkeit

Onlinesperrung und Statusprüfung für Zertifikate stehen nicht zur Verfügung.

4.11 Beendigung der Zertifikatsnutzung durch den Zertifikatsnehmer

Eine Beendigung der Zertifikatsnutzung durch die Zertifikatsnehmer erfolgt

- durch die Sperrung oder

- indem kein neues Zertifikat nach dem Ablauf beantragt wird.

4.12 Schlüsselhinterlegung und –wiederherstellung

(Nichtzutreffend). Hinterlegung wird nicht angeboten.

5.Nicht technische Sicherheitsmaßnahmen

Die CAs müssen vor ihrer Betriebsaufnahme ein ISMS (Information Security Management System) einführen. Die Sicherheitsmaßnahmen sind in einem nicht öffentlichen Sicherheitskonzept und den dazugehörigen Anlagen sowie dem Standortkonzept zusammengefasst.

Das Sicherheitskonzept muss

- administrative, organisatorische, technische und infrastrukturelle Sicherungsmaßnahmen beinhalten, die der Bedeutung der Zertifikatsdaten und des Zertifikatsmanagement-Prozesses entsprechen.
- den aktuellen Stand der Technik und die Kosten bestimmter Maßnahmen berücksichtigen und ein angemessenes Sicherheitsniveau für die Schäden, die entstehen könnten und den Schutzbedarf der Daten, die geschützt werden sollen, gewährleisten.
- eine Risikobewertung beinhalten, die interne und externe Bedrohungen aufführt, die zu unautorisierten Zugriffen, Veröffentlichungen, Missbrauch, Austausch oder Zerstörung von Zertifikatsdaten oder des Zertifikatsmanagement-Prozesses führen können.

Bewertet werden muss im Rahmen der Risikobewertung die Eintrittswahrscheinlichkeit und der mögliche Schaden dieser Bedrohungen betrachtet werden.

Das Sicherheitskonzept für den Zertifikatsmanagement-Prozess muss insbesondere auch folgende Aspekte berücksichtigen:

- Physikalische Sicherheit und umweltbezogene Maßnahmen.
- Systemintegritätsmaßnahmen, Konfigurationsmanagement, Erhaltung der Integrität von vertrauenswürdigem Code, Malware-Erkennung und Vorsichtsmaßnahmen.
- Benutzermanagement, eine eigene Vergabe von vertrauenswürdigen Rollen, Ausbildung, Sensibilisierung und Fortbildung.

5.1 Physikalische Kontrollen

Die CA muss Maßnahmen beschreiben, die den Schutz der Infrastruktur erhöhen.

5.1.1. Standort und bauliche Maßnahmen

Die CA wird innerhalb eines zugangsgesicherten Bereichs in einem weiteren Sicherheitsbereich betrieben. Der Sicherheitsbereich ist an eine Alarmsystem angeschlossen. Standorte und die technischen und baulichen Maßnahmen zum Schutz der CA sind detailliert in den nicht zur Veröffentlichung vorgesehenen Standortkonzepten beschrieben. Dies gilt auch für die folgenden Punkte.

5.1.2 Physikalischer Zutritt

Zutritt erfolgt über ein mehrstufiges Zugangssystem. Dabei werden folgende Anforderungen berücksichtigt:

- Das Gebäude ist von einem Pförtner in der Kernarbeitszeit besetzt.
- Alle Zugänge sind nur über Authentisierung zu öffnen.
- Externe Gäste werden durch Mitarbeiter am Empfang abgeholt.
- Nur autorisiertes Personal hat Zutritt zu den sicherheitskritischen Bereichen, um eine Kompromittierung durch unautorisierte Zugriffe zu verhindern.
- Nur Zutrittsberechtigungen, die betrieblich notwendig sind, werden erteilt.
- Berechtigung werden regelmäßig überprüft. Zutritte werden protokolliert.

Zutritt zum Sicherheitsbereich:

Die Räume in denen die Technik untergebracht sind alarmgesichert. Chipkarten, Schlüssel und die Zutrittsanlage werden intern verwaltet.

Die TC-Technik befindet sich in einem abgeschlossenen Sicherheitsbereich mit eigener Zutrittskontrollanlage und Alarmanlage. Die Zutrittskontrollanlage ist zusätzlich zu der Zutrittsanlage des Gebäudes installiert.

Um den Sicherheitsbereich zu betreten, müssen somit zwei Zutrittskontrollsysteme durchlaufen werden:

- Die Berechtigungsvergaben und Zutritte werden dokumentiert. Die Zutrittsberechtigungen werden regelmäßig überprüft sind Teil eines Rollenkonzepts.
- Der Server steht in einem abgesicherten Serverschrank. Der Zugriff auf die eingesetzten Hardware Security Module (HSMs) wird über Vieraugenprinzip und Smartcards abgesichert.
- Die Zutrittsberechtigungen sowie die zu deren Umsetzung notwendigen Chipkarten und Schlüssel werden ausgegeben bei Bedarf und sind individualisiert in Listen festgehalten. Die Ausgabe wird ebenfalls dokumentiert.

5.1.3 Klimatisierung und Stromversorgung

Die Maßnahmen zur Stromversorgung und Klimatisierung sind auf geforderte Verfügbarkeit der PKI und der technischen Geräte vor Ort abgestimmt.

5.1.4 Wasserschäden

Die Niederlassung verfügt über einen angemessenen Schutz vor Wasserschäden. Stehende oder fließenden Gewässer befinden sich nicht in der Nähe der Niederlassung.

5.1.5 Brandschutz

Das Gebäude besitzt mehreren Brandabschnitte. Die Räume sind mit Brand- und Rauchmeldern ausgerüstet werden. Sicherungen und Geräte befinden sich in unterschiedlichen Brandabschnitten.

5.1.6 Aufbewahrung von Datenträgern

Datenträger mit kritischen Betriebsdaten sind vor Umwelteinflüssen geschützt gelagert. Hierfür wird ein Sicherheitsbereich eines anderen Brandabschnitts genutzt. Der Sicherheitsbereich in einem anderen Brandabschnitt hat eine eigene physische Zutrittskontrolle. Archiv – und Sicherungen,

werden nur Räumen gelagert, die mit entsprechenden physischen und logischen Zutrittskontrollen versehen sind und Schutz vor Wasser-, Brand- und elektromagnetischen Schäden bieten.

5.1.7 Entsorgung

Dokumente und Datenträger werden fachgerecht entsorgt. Die Sicherheit der Daten ist insoweit gewährleistet. Die Entsorgung muss protokolliert werden.

5.1.8 Externe Sicherung

Von kritischen Daten werden Sicherheitskopien erzeugt und an einem anderen Standort oder in einem zweiten Brandabschnitt verschlüsselt gesichert (s. hierzu auch Abschnitt 5.1.6).

5.2 Organisatorische Maßnahmen

5.2.1 Vertrauenswürdige Rollen

Alle Rollen, die innerhalb der CA kritische Funktionen wahrnehmen und die Vertrauenswürdigkeit der CA einschränken können, werden als vertrauenswürdige Rollen bezeichnet.

Dies sind:

- Teilnehmerservice (TS)
- Registrator (RA)
- Zertifizierer (Z)
- HSM-Administrator (HA)
- Key-Manager (KM)
- System Operator (SO)

Diese Rollen müssen in im Rollenkonzept beschrieben werden und dürfen nur mit geeigneten und vertrauenswürdigen Personen besetzt werden. Die Besetzung erfolgt über eine dokumentierte Rollenzuweisung.

5.2.2 Anzahl der für eine Aufgabe erforderlichen Personen

Kritische Aufgaben, insbesondere Arbeiten mit dem privaten Schlüssel der CA, werden im Vier-Augen-Prinzip durch Personen in einer vertrauenswürdigen Rolle durchgeführt. Dies gilt auch für Arbeiten an Komponenten wie HSM und CA-Systemen bzw. Systemen auf denen Schlüssel erstellt werden.

5.2.3 Identifizierung von Mitarbeitern für die Ausübung von Rollen

Mitarbeiter, die vertrauenswürdige Rollen übernehmen, sind identifiziert und entsprechend 5.3.2 überprüft.

Es muss sichergestellt sein, dass die Mitarbeiter identifiziert, werden bevor sie:

- Zugriff auf kritische Systeme erhalten
- Zugang zu Einrichtungen erhalten.

5.2.4 Aufgabentrennung und Rollen

Eine Aufgabentrennung liegt vor. Ein Mitarbeiter darf nur innerhalb einer dieser Bereiche eine Rolle übernehmen.

5.3 Personal

5.3.1 Anforderungen an Qualifikation, Erfahrung und Sicherheitsüberprüfung

Alle Personen in der Zertifikatsverwaltung müssen vertrauenswürdig sein und über die notwendige Fachkunde und Erfahrung verfügen.

Für die Tätigkeit in der PKI findet eine Einarbeitung durch erfahrene Mitarbeiter und Mitarbeiterinnen statt.

5.3.2 Sicherheitsüberprüfung

Personen, die eine vertrauenswürdige Rolle übernehmen sollen, legen ein Führungszeugnis gemäß Bundeszentralregistergesetz BZRG § 30 oder vergleichbares vor. Stehen Einträge einer Übernahme der Rolle entgegen, so muss die Rollenübernahme abgelehnt werden. Die CA kann weitere Prüfungen vornehmen. Die Überprüfung des Führungszeugnisses (oder vergleichbar) sollt nach drei Jahren erneuert werden.

5.3.3 Schulung und Fortbildung

Das Personal wird geschult, bevor es entsprechende Rollen und Tätigkeiten übernimmt.

Diese Schulung muss mindestens Basiswissen vermitteln zu

- Public Key Infrastrukturen und Anforderungen an PKIs inklusive Key-Management
- zu Manipulationsmöglichkeiten von Dokumenten, Verifikationsprozesses und Bedrohungen durch Phishing und Social Engineering
- zum Datenschutz, und
- Informationen an das Personal weitergeben zur Meldung und zum Umgang mit Störungen.

5.3.4 Nachschulungen

Das Personal muss regelmäßig nachgeschult werden. Insbesondere Personen in vertrauenswürdigen Rollen müssen auf dem entsprechenden Wissensstand gehalten werden. Bei Änderungen bei Prozessen und Anforderungen für die PKI sollte eine Nachschulung innerhalb von 3-6 Monaten durchgeführt werden. Aufgrund von wöchentlichen Abstimmungsmeetings ist derzeit ein beständiger Informationsfluss und Knowhowtransfer gesichert.

5.3.5 Arbeitsplatzrotation

Es muss sichergestellt werden, dass durch einen Wechsel eines Arbeitsplatzes in unterschiedlichen Bereichen kein Rollenausschluss umgangen werden kann, indem mehrere Rollen übernommen werden. Dies muss in den Sicherheitskonzepten und Rollenkonzepten betrachtet werden.

5.3.6 Sanktionen bei unbefugten Handlungen

Unbefugte Handlungen werden protokolliert und sanktioniert und je nach Schwere wird die Handlung zu einem Ausschluss der Person aus dem CA-Betrieb führen.

5.3.7 Anforderungen an unabhängige Auftragnehmer

(Nichtzutreffend für PCA und Sub-CA)

5.3.8 Dokumentation, Schulungsunterlagen und Verfahrensanweisungen

Den Rolleninhabern haben ausreichende Dokumentationen (Schulungen und Verfahrensanweisungen) zur Erledigung ihrer Tätigkeiten zur Verfügung gestellt bekommen.

5.4 Protokollierung und Aufzeichnung von Ereignissen

5.4.1 Auszeichnung von Ereignissen

5.4.1.1 Lebenszyklus von PCA und CA-Schlüsselpaaren

Für das Lifecycle-Management generell von Zertifikaten werden die folgenden Ereignisse protokolliert:

- Erstellung und Sperrung von Zertifikaten
- Schlüsselwechsel
- Annahme oder Ablehnung von Zertifikatsaufträgen
- Ausstellung eines Zertifikates
- Erzeugung und Übertragung von Gesamtlisten
- Erzeugung von Sperrlisten.

5.4.1.2 Sonstige sicherheitsrelevante Ereignisse

Zusätzlich werden für den Betrieb der Infrastruktur sicherheitsrelevanten Ereignisse protokolliert. Dies beinhaltet mindestens die folgenden Ereignisse:

- Erfolgreiche und erfolglose Zugriffsversuche auf Systeme der PKI
- Durchgeführte Aktionen an und durch die PKI
- Änderungen am Sicherheitsprofil
- Systemabstürze, Hardware-Ausfälle und andere Anomalien
- Firewall- und Router-Aktivitäten hinsichtlich Internetserver
- Zutritt und Verlassen der gesicherten Umgebung.

5.4.2 Untersuchung von Protokollen

Protokoll- und Logdateien werden auf sicherheit – und betriebsrelevante Ereignisse untersucht.

5.4.3 Aufbewahrungszeitraum für Audit-Protokolle

Die Protokolle und Datenbankeinträge zu Protokollierungszwecken müssen sechs (6) Jahre aufbewahrt werden.

5.4.4 Schutz der Audit-Protokolle

Die Protokolldaten werden zusammen mit der Datenbank gesichert. Nachträgliche Änderungen sind nicht möglich insbesondere nicht über die CA-Oberfläche.

5.4.5 Sicherungsverfahren für Audit-Protokolle

Auditprotokolle werden bedarfsweise gesichert.

5.4.6 Audit-Protokolle-Erfassungssystem

Protokoll-Datensätze werden direkt in dem CA-System und Datenbankserver erzeugt. Manuelle Dokumentationen von Prozessen und Ereignissen werden von den Mitarbeitern mittels Protokolle und Checklisten dokumentiert.

5.4.7 Benachrichtigung des Ereignisauslösenden Subjekts

Mitteilung über Überwachungssysteme werden je nach Art des Ereignisses an die jeweils verantwortlichen Mitarbeiter zur Bewertung weitergeleitet.

5.4.8 Schwachstellenprüfung

Die CA überprüft ihre Systeme regelmäßig quartalsmäßig auf Schwachstellen untersuchen. Bekanntwerdende kritische auftretende Fehler für Softwarepaket werden anlassbedingt sofort überprüft und behoben.

Das Sicherheitskonzept muss eine jährliche aktualisierte Risikoanalyse beinhalten, die die vorhersehbaren internen und externen Bedrohungen identifiziert, die zu einem unautorisierten Zugriff, Veröffentlichung, Missbrauch, Austausch oder Zerstörung von Zertifikatsdaten oder des Zertifikatsmanagement-Prozesses führen können. Anlass bedingt muss die Aktualisierung früher gemacht werden.

Die Rahmen der Risikoanalyse und der regelmäßigen Schwachstellenbewertung muss ebenfalls überprüfen werden, ob Vorgaben, Verfahren, Informationsverarbeitende Systeme, Technik und andere Zusammenstellungen, welche die CA nutzt, ausreichend sind, um den Bedrohungen wirksam zu begegnen.

5.5. Datenarchivierung

5.5.1 Art der archivierten Datensätze

Die PCA und CA muss mindestens die folgenden Daten archivieren:

- CPS, CP, AGB und vertragliche Unterlagen
- Zertifizierungsunterlagen und Auditberichte
- Systemkonfigurationen
- Antragsunterlagen inkl. Prüfungen in digitaler Form
- Ausgestellte Zertifikate
- Sperranträge
- Sicherheitskonzeption
- Sicherheitsvorfälle
- Protokolldaten

Die Daten werden in der Datenbank und vom CA-Server gesichert.

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Die vorgenannten Aufzeichnungen (Arten der archivierten Datensätze) müssen sechs (6) Jahre aufbewahrt werden. Andere weitergehende gesetzliche Anforderungen müssen eingehalten werden. Dies gilt auch für die 10-jährige Löschfristen für den Nachweis von Geschäftsvorfällen nach § 257 HGV und § 147 AO.

5.5.3 Schutz von Archiven

Die CA stellt sicher, dass nur autorisierte und vertrauenswürdige Personen Zutritt zu Archiven erhalten. Es gelten die gleichen Zugangsanforderungen für die Sicherungen wie für die neuen Daten.

5.5.4 Sicherungsverfahren für Archive

Archivdaten werden gegen unbefugte Lesezugriffe, Änderungen, Löschungen oder andere Manipulationen geschützt. Die Haltbarkeit der Sicherungsdaten und Sicherungsmedien sowie der genutzten Datenformate muss dabei sichergestellt werden.

5.5.5 Anforderungen an Zeitstempel von Datensätzen

Alle Ereignisse, die durch die Datensätze (s. Abschnitt 5.5.1) dokumentiert werden, enthalten Informationen zu Datum und Uhrzeit.

5.5.6 Verfahren zur Beschaffung und Überprüfung von Archivinformationen

Nur autorisiertes und vertrauenswürdiges Personal erhält Zutritt zu Archiven und Zugang bzw. Zugriff zu Archivdaten.

5.6 Schlüsselwechsel

Beim Schlüsselwechsel von PCA und Sub-CA ist die Erzeugung der neuen Schlüssel und die Erstellung der Zertifikate zu dokumentieren. An dem Schlüsselwechsel nehmen nur authentifizierte Mitarbeiter teil entsprechend ihren Rollen aus dem Rollenkonzept.

Die erstellten neuen Zertifikate und die Fingerprints sind zu veröffentlichen. Siehe zur Veröffentlichung hierzu auch Abschnitt 2.2..

Der Schlüsselwechsel für die PCA und die Zertifizierungsverfahren erfolgen stets im Vier-Augen-Prinzip.

5.7 Kompromittierung und Wiederherstellung des Betriebes

Die CA‘s müssen über eine Geschäftserhaltungsplanung (business continuing plan) verfügen, um den Geschäftsbetrieb bei Ausfällen oder Krisensituationen zu gewährleisten.

Die Planung wird aktualisiert und einem regelmäßigen Review unterzogen und durch Notfallübungen getestet.

Im Fall der Kompromittierung privater Schlüssel von PCA und Sub-CA ist dies unverzüglich den betroffenen Zertifizierungsstellen mitzuteilen.

Die betroffenen Sub-CA Zertifikate der Zertifizierungsstellen sind zu sperren und die entsprechende Sperrliste unverzüglich zu veröffentlichen. Dies gilt auch für die durch die Zertifizierungsstellen erstellten Endnutzer-Zertifikate. Die Endnutzer müssen hierfür über die Webseiten informiert werden.

Die PKI nutzt das Whitelist-Verfahren. Werktäglich werden Gesamtlisten und LDIF-Dateien bereitgestellt mit den gültigen PCA, CA und Endnutzerzertifikaten. Eine täglich aktuelle Verteilung der gültigen Zertifikate ist somit gewährleistet.

Neue Schlüssel und Zertifikate sind zu erzeugen und die Erstellung zu dokumentieren und zu veröffentlichen.

5.7.1 Umgang mit Störungen und Kompromittierungen

Der Geschäftserhaltungsplan (business continuing plan) muss folgende Aspekte beinhalten:

- die Bedingungen für die Einleitung der beschriebenen Maßnahmen
- die Notfallprozesse (Fallback)
- Wiederaufnahmepläne
- Sensibilisierung und Wissensanforderungen
- Vorgaben für die Wiederherstellungszeiten
- Regelmäßiges Testen möglicher Fälle
- Einen Zeitplan zur Wiederherstellung bzw. Wiederaufnahme des Geschäftsbetriebes nach einem Fehler oder Ausfall.
- Eine Anforderung zur Lagerung von kritischem kryptografischem Material (e.g. HSM) an einem alternativen Ort.
- Die Festlegung von akzeptablen Zeiten für Systemausfall und Wiederherstellung.
- Die Festlegung von Backupzyklen für essenzielle Geschäftsinformationen und Software.
- Die Entfernung von Wiederherstellungsstandorten und dem Hauptstandort der CA.
- Planungsunterlagen für die Sicherung der Geschäftsräume während eines Desasters und der Wiederherstellung an diesem Standort oder an einem anderen Standort.

5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln

Bei einer Kompromittierung des privaten Schlüssels einer CA muss der Vorfall unmittelbar untersucht und gegebenenfalls die notwendigen Schritte der Sperrung durch die PCA eingeleitet werden.

Die Endteilnehmer werden von der CA über die mögliche Kompromittierung durch die Webseite der PCA bzw. Sub-CA informiert.

Die PKI nutzt das Whitelist-Verfahren. Es werden daher täglich nur die gültigen PCA, CA und Endnutzerzertifikate mit den täglichen Lieferungen der Gesamtlisten und LDIF-Dateien verteilt und veröffentlicht.

Die betroffene CA wird mit einem neuerstellen Schlüsselpaar neu aufgesetzt. Das Zertifikat der neuen Zertifizierungsstelle ist zu veröffentlichen und die zuvor gestellten Zertifikate der Zertifikatsnehmer sind neu auszustellen.

Das Verfahren ist ebenfalls anzuwenden auf die Kompromittierung der PCA.

5.7.4 Geschäftskontinuität nach einem Notfall

Die PCA muss einen Notfallplan entwickeln, implementieren und testen, um die Auswirkungen von Katastrophen und sonstigen Beeinträchtigungen abzufangen und die kritischen Geschäftsprozesse so schnell wie möglich wiederherzustellen.

Die Wiederherstellung deckt alle Geschäftsprozesse, Komponenten, Systeme und Dienste der PCA und der Sub-CA ab.

Dieses Wiederherstellungskonzept wird jährlich überprüft und entsprechend aktualisiert, um im Fall einer Beeinträchtigung aller Geschäftsprozesse gezielt reagieren zu können und den Betrieb wieder herzustellen (siehe hierzu auch Abschnitt 5.7.1).

5.8 Einstellung des PCA, CA oder RA-Betriebes

Die den Betrieb einstellende PCA und deren CA muss die Maßnahmen für die Beendigung des Betriebs in einem Betriebseinstellungskonzept beschreiben.

Dies umfasst insbesondere die Mitteilung der Betriebseinstellung.

Eine Erklärung für die Übernahme oder Bereitstellung von Geldmitteln für die Kosten der Einstellung, Abwicklung oder Übertragung der gültigen Zertifikate auf eine andere CA bzw. PKI ist zu regeln.

Das Einstellungskonzept sollte ferner folgende konkrete Regelungen enthalten:

- die Fortführung des Sperrservice
- die Sperrung von ausgegebenen CA-Zertifikaten
- die Übergangvereinbarung auf eine Nachfolge-CA ansonsten Planung der Sperrung aller Zertifikate
- die Regelungen zur Archivierung der Unterlagen der CA.

6.Technische Sicherheitsmaßnahmen

6.1 Generierung und Installation von Schlüsselpaaren

6.1.1. Generierung von Schlüsselpaaren der PCA und CA

Die Erzeugung von PCA und CA-Schlüsseln und die Erstellung der Zertifikate werden in einer gesicherten Umgebung auf Hardware Security Modulen (HSM) durchgeführt.

Bei der Schlüsselerzeugung wird das Rollenkonzepts des TrustCenter und das 4-Augen-Prinzip beachtet. Der Prozess der Schlüsselzeremonie wird dokumentiert.

6.1.1.2 Generierung von RA- Schlüsselpaaren

(Nichtzutreffend)

6.1.1.3 Generierung von Subscriber-Schlüsselpaaren (EE-Zertifikate)

(Nichtzutreffend für die PCA und CA)

6.1.2 Bereitstellung des privaten Schlüssels an Zertifikatsnehmer

(Nichtzutreffend)

Private Schlüssel werden weder für Zertifikatsnehmer erstellt, verwahrt noch ausgeliefert.

6.1.3 Bereitstellung des öffentlichen Schlüssels an die Zertifizierungsstelle

Die Schlüsselpaare für die PCA und die Sub-CA Zertifikate werden direkt in der gesicherten Umgebung erstellt. Eine externe Übermittlung an die Zertifizierungsstelle ist nicht notwendig.

6.1.4 Bereitstellung der öffentlichen PCA und CA-Schlüssels

Eine Bereitstellung kann darüber durch Veröffentlichung auf den Webseiten der nachgeordneten Zertifizierungsstellen in öffentlichen Schlüsselverzeichnisse oder in einem LDAP-Verzeichnis der Zertifizierungsstellen (ITSG) erfolgen.

6.1.5 Algorithmen und Schlüssellängen

Hierzu wird auf die Vorgaben aus der Anlage 16 „Gemeinsame Grundsätze Technik“ verwiesen.

Die RSA-Schlüssellänge beträgt:

- PCA-Schlüssel 4096 Bit (Standard); nach gesonderter Festlegung auch größer
- CA-Schlüssel 4096 Bit (Standard); nach gesonderter Festlegung auch größer
- Teilnehmer-Schlüssel 4096 Bit (Standard)

Signaturhashalgorithmus (SHA)	Message Digest“	SHA-256	[OID 2.16.840.1.101.3.4.2.1]	RFC8017	Anlage 16
Signatur-Algorithmus	Signature Algorithms	id-RSASSA-PSS	[OID 1.2.840.113549.1.1.10]	BSI-TR3116-4	Anlage 16
Verschlüsselungsalgorithmus (Nachrichtenschlüssel)	Key Encryption Algorithmus	id-RSAES-OAEP	[OID 1.2.840.113549.1.1.7]	RFC8017	Anlage16-2.1.2
rsaEncryption PCA 4096 Bits CA-Schlüssel 4096 Bits Teilnehmer 4096 Bits	Subject Public Key Algorithmus (Verschlüsselung)	id-aes256-CBS	[OID 1.2.840.113549.1.1.1]	RFC3565	Anlage 16 - 2.13

6.1.5.1 PCA -Zertifikate

Die Schlüssellänge der Root-CA-Zertifikate:

- Schlüssellänge: RSA 4096 Bits [OID 2.16.840.1.101.3.4.2.1]
- Signaturhashalgorithmus: SHA256
- Signaturalgorithmus: id-RSASSA-PSS [OID 1.2.840.113549.1.1.10]
- Nachrichtenschlüssel: d-RSAES-OAEP [OID 1.2.840.113549.1.1.7]
- rsaEncryption [OID 1.2.840.113549.1.1.1]

6.1.5.2 Subordinate-CA Zertifikate

Die Schlüssellänge für Sub-CA-Zertifikate:

- Schlüssellänge: RSA 4096 Bits [OID 2.16.840.1.101.3.4.2.1]
- Signaturhashalgorithmus: SHA256

- Signaturalgorithmus: id-RSASSA-PSS [OID 1.2.840.113549.1.1.10]
- Nachrichtenschlüssel: d-RSAES-OAEP [OID 1.2.840.113549.1.1.7]
- rsaEncryption [OID 1.2.840.113549.1.1.1]

6.1.6 Generierung öffentlicher Schlüsselparameter und Qualitätskontrolle

Die Parameter der Schlüssel von Root CA-, Sub-CA- und EE-Zertifikaten und ggf. anzuwendende Qualitätskontrollen sind in der Anlage 16 „Gemeinsame Grundsätze Technik“ festgelegt.

6.1.7 Bestimmung der Schlüsselverwendung

Private PCA-Schlüssel dürfen ausschließlich zum Signieren von Sub-CA-Zertifikaten und Sperrlisten für die Sub-CA Zertifikate verwendet werden.

- Zertifikatsignatur,
- Offline-Signieren der Zertifikatsperrliste,
- Signieren der Zertifikatsperrliste (06).

Die privaten *Sub-CA-Schlüssel* dürfen (Anlage 16 insb. Abschnitt 2.2.7)

- Zertifikatsignatur,
- Offline-Signieren der Zertifikatsperrliste,
- Signieren der Zertifikatsperrliste (06).
- Typ des Antragstellers=Zertifizierungsstelle
- (*PathLenConstraint*) Einschränkung der Pfadlänge auf 0; nur Benutzerzertifikate können ausgestellt werden.

6.2 Schutz privater Schlüssel und technische Kontrollen kryptografischer Module

6.2.1 Standards und Kontrollen für kryptografische Module

Die privaten Schlüssel der Root-CAs werden nur auf sicherheitsüberprüften Hardware Security Modulen (HSM) abgelegt. Die Module werden gegen technische und organisatorische Manipulationen geschützt.

6.2.2 Vier-Augen-Prinzip bei privaten Schlüsseln

Die Kontrolle von privaten Root Schlüsseln ist durch das vier Augen-Prinzip geschützt. Die Ausführung von Aktionen wird technisch oder / und organisatorisch beschränkt. Für die Durchführung einer Schlüsselzeremonie sind daher zwei Key-Manager erforderlich.

6.2.3 Hinterlegung von privaten Schlüsseln

(Nichtzutreffend) Eine Hinterlegung von privaten Schlüsseln bei Treuhändern wird nicht durchgeführt.

6.2.4 Sicherung (Key-Backup) von privaten Schlüsseln

Die privaten Schlüssel werden im Rahmen der Schlüsselzeremonie von den Key-Managern in einem mit dem MBK verschlüsselten Backup entsprechend dem Vier-Augenprinzip und dem Rollenkonzept

des TrustCenters gesichert. Der Backup privaten Schlüssel dürfen nur von Key-Managern im Rahmen einer Schlüsselzeremonie erstellt werden. Die Sicherung wird protokolliert. Die mit dem MasterBackupKey (MBK) des HSM verschlüsselten Backups werden in einem Sicherheitsbereich gesichert und können nur im vier Augenprinzip auf einen HSM zurückgespielt werden.

6.2.5 Archivierung von privaten Schlüsseln

Nach dem Ende der Gültigkeit von PCA und CA -Schlüsseln sind die Vorgaben des Löschkonzeptes umzusetzen und die Schlüssel zu löschen. Die privaten Schlüssel der CA werden nach Ablauf oder Sperrung noch 10 Jahre aufbewahrt.

6.2.6 Übertragung privater Schlüssel in oder von einem kryptografischen Modul

Private Schlüssel liegen zu keinem Zeitpunkt unverschlüsselt vor. Die Tätigkeit des Backups mittels MBK wird im Rahmen einer Schlüsselzeremonie im Vier-Augenprinzip durchgeführt. Die Übertragung von privaten Schlüsseln erfolgt nur verschlüsselt mit dem MBK.

6.2.7 Speicherung privater Schlüssel auf kryptografischen Modulen

Schlüsselpaare werden in einem kryptografischen gesicherten Modul (Hardware Security Module) gespeichert.

6.2.8 Aktivierung privater PCA-Schlüssel auf kryptografischen Modulen

Die Root-CA-Schlüssel müssen im Vier-Augenprinzip erstellt werden. Mit der Erstellung im kryptographischen Modul wird der Schlüssel aktiviert.

6.2.9 Aktivierung privater Sub-CA-Schlüssel auf kryptografischen Modulen

(Nichtzutreffend)

6.2.10 Vernichtung privater Schlüssel

Nach Ablauf der Gültigkeit oder Sperrung des privaten PCA oder CA-Schlüssel werden diese nach einer Aufbewahrungsrist von 10 Jahren gelöscht. Das Löschen erfolgt im Rahmen einer Key-Zeremonie und im Vier-Augenprinzip.

6.3 Aspekte zur Verwaltung von Schlüsselpaaren

6.3.1 Archivierung von öffentlichen Schlüsseln

Die Archivierung von PCA und CA-Schlüsseln ist immer durch Mehrpersonen (2 Personen) durchzuführen und zu dokumentieren.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

- PCA CA Zertifikat 7 Jahre
- CA–Zertifikat 5 Jahre
- Benutzerzertifikate (Dale und AGV) 3 Jahre
- Benutzerzertifikate (DKTIG) 2 Jahre

7 Profile von Zertifikaten und Sperrlisten

7.1 Versionsnummer

Die Zertifikate werden entsprechen des X.509v3 Standard ausgestellt.

7.2 X.509v3 Zertifikate und Erweiterungen

Der x.509v3 Standard beinhaltet eine Vielzahl an Zertifikatserweiterungen. Die Zertifikate und Sperrlisten müssen, die für die Prüfung der Gültigkeit notwendigen Informationen enthalten. Eine Abstimmung zwischen allen am Verfahren Beteiligten ist bei Änderungen der Zertifikatserweiterungen notwendig.

Als Basis gelten die Festlegungen der Profile für Zertifikate und Sperrlisten nach dem MTTv2 – Spezifikationen.

7.2.1 CA-Zertifikate enthalten folgende Erweiterungen

Key Usage

- cert sign, crl sign
- Signieren von Zertifikaten und Sperrlisten

Basic Constraints

- Das Feld Basic Constraints ist eine optionale Datenstruktur, die das Zertifikat einer Rolle zuordnet.
- Die Zertifikate der CA und PCA müssen die Parameter CA= True enthalten.
- Die Teilnehmerzertifikate müssen die CA=FALSE enthalten.
- Pfadlängenbeschränkung=0

Subject Key Identifier

- Das Feld SubjectKeyIdentifier (SKI) ist eine optionale Datenstruktur, die einen Prüfwert des öffentlichen Schlüssels eines Zertifikats erhält.

Bei optionaler Verwendung gilt folgende Datenstruktur

- *SubjctKeyIdentifier* ::= *KeyIdentifier*
- Die Erweiterung muss in allen CA-Zertifikaten enthalten sein.

7.2.2 Benutzerzertifikate

Hinsichtlich Details zu den Benutzerzertifikate wird auf die Abschnitte in der Anlage 16 Abschnitt 4.4.9 u.4.4.10 verwiesen.

7.3 Sperrlistenprofile

Es wird für weitere Details auf den Abschnitt 5.9.5 „Sperrliste“ in der Anlage 16 verwiesen.

8 Konformitätsprüfung

Die Verfahren und Prozesse der Zertifizierungs – und der Registrierungsstelle werden regelmäßig und gegebenenfalls anlassbezogen überprüft. Die inhaltlichen Ergebnisse der internen Audits werden nicht veröffentlicht.

8.1 Frequenz und Umstände der Überprüfung

Interne und externe Audits werden in regelmäßig durchgeführt. Jährlich werden für die Trustcenter die ISO 27001: 2017 Audits durchgeführt. Daneben werden interne Audits entsprechend einem übergreifenden Auditplan durchgeführt.

8.2 Identität und Qualifikation des Prüfers

Die Prüfer verfügen über die notwendigen Kenntnisse auf dem Gebiet der Public Key Infrastructure (PKI), um die Prüfungen vornehmen zu können.

8.3 Verhältnis von Prüfer zu Überprüftem

Die Prüfer dürfen nicht in den Produktionsprozess eingebunden sein.

8.4 Überprüfte Bereiche

Es können alle für die PKI relevanten Bereiche überprüft werden. Die Prüfungsinhalte obliegen dem Prüfer.

8.5 Mängelbeseitigung

Mängel müssen entsprechend einer zu treffenden Abstimmung zwischen Zertifizierungsstelle und Prüfer zeitnah beseitigt werden. Die Prüfer werden über die Beseitigung der Mängel informiert.

8.6 Veröffentlichung der Ergebnisse

Eine externe Veröffentlichung der Prüfungsergebnisse z.B. auf der Webseite ist nicht vorgesehen.

9 Weitere geschäftliche und rechtliche Regelungen

9.1 Gebühren

Detaillierte Informationen für die PCA und CA finden sich in den Verträgen mit den Auftraggebern.

9.2 Finanzielle Verantwortung

Risiken, die aus der Haftung für eine CA entstehen können, werden durch die Auftraggeber abgedeckt. Dies kann auch mittels Haftpflichtversicherung geschehen.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Informationen und Dateien über Teilnehmer und Zertifikationsnehmer sind grundsätzlich vertrauliche Informationen.

Dieses gilt, soweit die Daten nicht direkt den Inhalt des Zertifikats betreffen. Einschränkung zur Vertraulichkeit (siehe Abschnitt 9.3.2).

9.3.2 Daten und Informationen in den herausgegebenen Zertifikaten

Sperrlisten, insbesondere Daten, die in den Zertifikaten enthalten sind, oder abgeleitete Daten, werden als nicht vertraulich eingestuft.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Das TrustCenter trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen.

9.4 Schutz personenbezogener Daten

Die Speicherung und Verarbeitung von personenbezogenen Daten richtet sich nach den gesetzlichen Datenschutzbestimmungen.

Daten über Zertifikatsnehmer und Teilnehmer werden vertraulich behandelt.

Die PKI trägt die Verantwortung für Maßnahmen zum Schutz personenbezogener Daten. Die Einschränkung bzw. Ausnahmen gemäß Abschnitt 9.3. der Policy gilt hier ebenfalls.

Die Zertifikatsnehmer stimmen der Nutzung von personenbezogenen Daten durch die PKI zu, soweit dies zur Leistungserbringung erforderlich ist. Darüber hinaus können alle Informationen veröffentlicht werden, die als nicht vertraulich behandelt werde. Näheres regelt die Datenschutzerklärung.

9.5 Urheberrechte

(Nichtzutreffend)

9.6 Verpflichtungen

Die PKI und die in die Registrierung eingebunden externen Stellen verpflichten sich den Bestimmungen dieses CPS zu folgen.

- Die Verpflichtung des Zertifikatsnehmers ist in Ziffer 4.5.1 geregelt
- Die Verpflichtung des Zertifikatsnutzers ist in Ziffer 4.5.2 geregelt.

9.7 Gewährleistung

Es besteht kein Anspruch darauf, dass die angebotenen Inhalte und Anwendungen stets störungsfrei verfügbar sind.

9.8 Haftungsbeschränkung

Die PKI-Betreiber haften unbeschränkt bei Vorsatz oder grober Fahrlässigkeit, für die Verletzung von Leben, Leib oder Gesundheit, nach den Vorschriften des Produkthaftungsgesetzes.

Bei leicht fahrlässiger Verletzung einer Pflicht, die wesentlich für die Erreichung der Zwecke dieser Nutzungsbedingungen ist (Kardinalpflicht), ist die Haftung der Höhe nach begrenzt auf den Schaden, der nach der Art des fraglichen Geschäfts vorhersehbar und typisch ist.

Die PKI-Betreiber haften nicht für Schäden, die darauf beruhen, dass es der Zertifikatsnehmer unterlassen hat, Datensicherungen durchzuführen und dadurch sicherzustellen, dass verlorengegangene Daten mit vertretbarem Aufwand wiederhergestellt werden können.

9.10 Inkrafttreten und Aufhebung

Dieses CPS tritt an dem Tag in Kraft, an dem es veröffentlicht wird. (gemäß Kapitel 2)
Dieses Dokument ist gültig, bis es durch eine neue veröffentlichte Version ersetzt wird oder Betrieb der PKI eingestellt wird.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

In dieser Zertifizierungsrichtlinie werden keine entsprechenden Regelungen getroffen.

9.12 Änderungen der Richtlinie

Änderungen des CPS werden rechtzeitig vor ihrem Inkrafttreten veröffentlicht.

9.13 Schiedsverfahren

Ein Schiedsverfahren wird nicht vereinbart.

9.14 Gerichtsstand

Der Gerichtstand für das von der DKTIG GmbH betriebene Trust Center ist Leipzig und der Gerichtstand für das von der ITSG GmbH betriebene Trust Center ist Offenbach am Main.

9.15 Geltendes Recht

Es gilt deutsches Recht.

9.16 Weitere Regelungen

Die Regelungen des CPS gelten zwischen der PKI und den Zertifikatsnehmern. Zertifikatsnehmer für die Sub-CA Zertifikate sind die Zertifizierungsstellen.

Sollten einzelne Bestimmungen dieser Zertifizierungsrichtlinie unwirksam sein oder werden, so lässt dies den übrigen Inhalt der Zertifizierungsrichtlinie unberührt. Auch eine Lücke berührt nicht die Wirksamkeit der Zertifizierungsrichtlinie im Übrigen. Anstelle der unwirksamen Bestimmung gilt diejenige wirksame Bestimmung als vereinbart, welche der ursprünglich gewollten am nächsten kommt oder nach Sinn und Zweck der Zertifizierungsrichtlinie geregelt worden wäre, sofern der Punkt bedacht worden wäre.

Die PKI übernimmt keine Haftung für die Verletzungen von Pflichten sowie für Verzug, Nichterfüllung im Rahmen dieses CPS, sofern das zugrundeliegende Ursache außerhalb ihrer Kontrolle (z.B. höhere Gewalt, Kriegshandlungen, Netzausfälle, Brände und Erdbeben sowie andere Katastrophen) liegt.

9.17 Andere Regelungen

- Anlage16 - Security Schnittstelle (SECON) zitiert als „Anlage16“
- BSI TR 3107-1 Elektronische Identitäten und Vertrauensdienste im E-Government
- BSI TR 3116-4 Kryptographische Vorgaben für Projekte der Bundesregierung

10 Abkürzungen

C	Country (Bestandteil des Distinguished Name)
CA	Certification Authority, Zertifizierungsinstanz
CN	Common Name (Bestandteil des Distinguished Name)
CP	Certificate Policy; Zertifizierungsrichtlinie einer PKI
CPS	Certification Practice Statement, Regelungen für den Zertifizierungsbetrieb
CRL	Sperrliste
(CRL) CDP	Extension Sperrlistenverteilungspunkte
DN	Distinguished Name
E-Mail	E-Mail-Adresse (Bestandteile des Distinguished Name)
HSM	Hardware Security Module (hier: Sicherung der Root CA und Sub CA Schlüssel)
http	Hypertext Transfer Protocol
https	Hypertext Transfer Protocol Secure
ISMS	Information Security Management Protokoll (Management System für Informationssicherheit
O	Organisation (Bestandteil des Distinguished Name)
OID	Object Identifier
OU	Organizational Unit (Bestandteil des Distinguished Name)
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PSE	Personal Security Environment
RA	Registration Authority, Registrierungsstelle
RFC	Request for Comment, Dokumente für weltweite Standardisierungen
Root-CA	Obererste Zertifizierungsinstanz einer PKI
S/MIME	Secure Multipurpose Internet Mail Extension