Tabelle Änderungshistorie

Version	Stand	Bearbeiter	Änderung / Kommentar
1.00	Stand 01.12.2023	Christoph Luxem	Initiale Version 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 einer Certificate Policy (CP) 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 und Zahlstellen, die über eine Betriebsnummer oder Zahlstellennummer verfügen*“ (s. 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 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 (CP)
Version:	1.0
Datum:	22.12.2023
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

Homepage: www.itsg.de

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 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 Zertifikatsnutzern und 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 Atos Information Technology GmbH betraut. Im Folgenden technischer Dienstleister genannt.

1.4 Verwendungen von Zertifikaten

1.4.1 Erlaubte Verwendung von Zertifikaten

Die folgenden Schlüsselverwendungen sind für die aufgeführten Policy Certification Authority und 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).

Die von den CAs erstellten Benutzerzertifikate enthalten keine Schlüsselverwendung und werden in der PKI für eine sichere Kommunikation im Gesundheitswesen und Sozialwesen genutzt. Die Schlüsselverwendung der Benutzerzertifikate ist in der Anlage 16 zur Security Schnittstelle (SECON) geregelt. Innerhalb der PKI werden folgende Schlüsselverwendungen angewendet:

- Signatur von elektronischen Nachrichten
- Verschlüsselung von elektronischen Nachrichten
- Authentisierung der Kommunikationspartner.

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 CP-Dokument

Das vorliegende CP-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)**
- Die Hotline ist unter der Telefonnummer 06104 947 36 – 403 in den folgenden Zeiten erreichbar:
- Montag bis Donnerstag: 08:30 – 12:30 Uhr und 13:30 – 17:00 Uhr
- Freitag: 08:30 – 14:00 Uhr
- Ausgenommen sind hessische und bundesweite Feiertage.
- E-Mail: kontakt@itsg.de
- URL.: https://www.itsg.de/kontakt/

Kontaktinformationen DKTIG GmbH:

- **Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH (DKTIG)**
- Humboldtstr. 9
- 04105 Leipzig
- Tel.: 0341 / 308951 – 0
- Fax: 0341 / 308951 – 25
- E-Mail: mail@dktig.de
- URL: https://dktig.de/kontakt/

1.5.3 Prüfung der Zertifizierungsrichtlinie

Die Certificate Policy (CP) 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 der CP wird von den beteiligten Partnern (siehe Beteiligte 1.1) sowie dem Spitzenverband der gesetzlichen Krankenkassen freigegeben.

1.5.4 Veröffentlichung der Zertifikatsrichtlinien

Die CP 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.

Jede *Certification Authority* muss für den Verzeichnisdienst den Zugriff auf Sperrdaten zur Verfügung stellen. Im von der PKI genutzten Whitelist-Verfahren werden täglich in Form der „Gesamtlisten“ und LDIF-Dateien für die LDAP -Verzeichnisse alle gültigen Zertifikate der Verfahren DALE, AGV und DKTIG für die Teilnehmer bereitgestellt. Hierzu gehören die gültigen PCA, CA und Benutzer-Zertifikate.

Die Gesamtlisten sind hierarchisch unter den gültigen PCA und Sub-CA Zertifikaten aufgebaut. Die Benutzerzertifikate befinden sich in den Gesamtlisten unter den CA-Zertifikaten, durch die sie bei der Erstellung signiert wurden.

Die Gesamtlisten können auf Homepages der beteiligten Zertifizierungsstellen geladen werden.

Daneben werden auch die Sperrlisten zusammen mit den Gesamtlisten an die Teilnehmer zur Verfügung gestellt:

Für das Arbeitgeberverfahren existieren folgende Schlüssellisten mit öffentlichen Teilnehmerschlüsseln:

- gesamt-pkcs.agv (alle Teilnehmerschlüssel)
- 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)
- 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)

Die Gesamtlisten enthalten nur die gültigen Zertifikate. Dies gilt ebenso für PCA und Sub-CA – Zertifikate. 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.

2.1.1 ITSG GmbH

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/antrag_ikbn.php

2.2.2 DKTIG GmbH

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

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 an Werktagen die Gesamtlisten auf dem aktuellen Stand.

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

2.4.1 ITSG Trust Center

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

- CA: ITSG TrustCenter für Arbeitgeber (AGV-Verfahren)
- CA: ITSG TrustCenter für sonstige Leistungserbringer (DALE-Verfahren)

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

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

(1) ZERTIFIKATE MIT RSASSA-PSS-SIGNATURALGORITHMUS

- 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

(2) ZERTIFIKATE MIT RSASSA-PSS-SIGNATURALGORITHMUS

- Seriennummer (dc): 85 / (hex): 55
- Gültigkeitszeitraum: 28.11.2023 bis 07.01.2029
- Signaturhashalgorithmus: SHA256
- Signaturalgorithmus: RSASSA-PSS
- Schlüssellänge: RSA 4096 Bits
- SHA1-Fingerprint: 1298f7e78a42133c52b6b4c01d0ee1703f75d6cb

CA-55.der (DER-Format, DER-codiert-binär X.509)
md5 Datei-Hash: 3aea276130ac9a116e659323a51e90b6

CA-55.pem (PEM-Format, Base64-codiert X.509)
md5 Datei-Hash: a2da71a95c031718eff8e934ebf75e91

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: 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

2.4.2 DKTIG Trust Center

PCA (Policy Certification Authority): Datenaustausch im Gesundheits- und Sozialwesen insb. Wurzelzertifikat der PCA: Organisation (o): 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

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

- 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)

(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) (siehe auch: 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 DNS für nachgeordneten Zertifizierungsstellen (siehe auch: 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 TrustCenter 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. Eine optionale Datenstruktur AuthorityKeyIdentifier (AKI) dient der eindeutigen Referenz auf das Ausstellerzertifikat.

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 und Arbeiten der PKI angewendet. Dies gilt insbesondere auch für Schlüsselzeremonie und Erstellung von 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. Es ist ausreichend, wenn die Erstellung der Sub-CA Zertifikate und PCA -

Wurzelzertifikate bei der Zertifizierungsstelle oder dem technischen Dienstleister in einem abgesicherten Bereich in einem Hardware Security Module (HSM) stattfinden.

3.2.2 Authentifizierung einer Organisation

Authentifiziert und identifiziert werden die genannten Ansprechpartner für ein Zertifikat. Die Authentifizierung einer Organisation durch das TrustCenter ist direkt nicht vorgesehen. Dies geschieht über die vorgelagerte Vergabestellen der Betriebsnummern, Absendernummern, Zahlstellennummern und Institutionskennziffer IK. Die Trust Center prüfen, ob die Nummer der antragstellenden Organisation zugeordnet werden darf. Dies kann bei der Antragstellung durch einen Freischaltcode erfolgen, der postalisch an die in einem Verzeichnis der Vergabestellen hinterlegte Adresse versendet wird.

3.2.3 Authentifizierung natürlicher Personen

Bei der Authentifizierung neuer natürliche Personen für die Auftraggeber und Sub-CA werden Verfahren zur Prüfung der Identität bei Änderungen der Ansprechpartner und Handelnden herangezogen. Die Vertrauenskette muss auf allen Stufen einschließlich bei der PCA und Zertifizierungsstellen eingehalten werden.

Zu den Verfahren gehören u.a.:

Personalausweis mit eID-Funktion

- Postidentifikationsverfahren.

3.2.4 Nicht überprüfte Zertifikatsnehmer Informationen

Im Rahmen der Vorbereitung der Zertifikatserneuerung und Schlüsselwechsel werden Zertifikatsnehmer und andere Teilnehmer überprüft.

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 CP).

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 zur Erstbeauftragung durchlaufen werden. Dies gilt insbesondere bei neuen Mitarbeitern (siehe auch Abschnitt 3.2.3 und 3.2.5).

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 oben Abschnitt 3.2.3.).

Autorisierte Personen ist der Ansprechpartner eines Zertifikates mit Unterschrift auf einem Sperrformular, oder ein Vorgesetzter des Ansprechpartners mit einem Nachweis.

4. Ablauforganisation (Betriebliche Anforderungen im Lebenszyklus von Zertifikaten)

4.1 Zertifikatsantrag

4.1.1 Antragsteller für ein 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.

4.1.2 Registrierungsprozess und Zuständigkeit

Die Beantragung von Zertifikaten erfolgt im Rahmen eines mehrstufigen Registrierungsprozess.

Es werden folgende Prüfungen vorgenommen:

- Berechtigung des Antragstellers
- Vollständigkeit und Korrektheit des Antrags
- Eindeutigkeit des DN
- Prüfung der Authentizität von Personen und Organisationen

Die Spitzenverbände der gesetzlichen Krankenkassen sehen hierfür eigene Prozesse und Prüfungen für neue Teilnehmer insb. neue Zertifizierungsstellen der PKI 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 nur von Key-Managern 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, die für eine Zertifikatserstellung benötigt werden und in der vorliegenden CP (siehe zum Zertifikatsantrag Abschnitt 4.1.3) aufgeführt werden, zur Verfügung stellen.

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 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.

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 bei Neuerstellung auf den Seiten der beteiligten TrustCenter veröffentlicht. Eine Veröffentlichung der Zertifikate in einem Verzeichnisdienst erfolgt mittels LDIF-Datei oder Gesamtlisten für die Teilnehmer der PKI. Siehe hierzu 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 CP erstellt werden, werden ausschließlich für die Nutzung in Zertifizierungsstellen ausgestellt (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 wird immer auch ein neues Schlüsselpaar im HSM (Hardware Security Module) erzeugt.

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 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.

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

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 täglich veröffentlicht auf der Webseite zum Download mit den 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 PCA 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 CP 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 (4.9.1) muss unverzüglich die Sperrung des Zertifikates veranlasst werden.

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 die Sperrung haben:

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 Teilnehmer bereitstehen. Die PKI beruht auf einem Whitelist-Verfahren. Die täglich erstellten Gesamtlisten enthalten alle gültigen PCA-, Sub-CA- und Benutzerzertifikate.

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 keine solche Sperrliste vor.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die Sperrlisten werden werktäglich zusammen mit den Gesamtlisten für die Teilnehmer der PKI bereitgestellt und übermittelt.
Die Sperrliste der PCA enthält die Sperrung untergeordneter Sub-CA Zertifikate der Zertifizierungsstellen.

4.9.9 Onlinesperrung und Statusprüfung von Zertifikaten

Online-Sperrungen und Statusprüfungen stehen nicht zur Verfügung. Die Zertifikatsnutzer erhalten nach Sperrungen mit den täglich neu erstellten Gesamtlisten nur gültige Zertifikate.
Gesperrte Zertifikate sind in Sperrlisten 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 oder 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 (nur ITSG) täglich den Teilnehmern zur Verfügung gestellt.

4.10.1 Betriebliche Vorgaben
Nichtzugreffend.

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
Nicht technische Sicherheitsmaßnahmen werden im CPS für die PCA beschrieben.

6.Technische Sicherheitsmaßnahmen
Nicht technische Sicherheitsmaßnahmen werden im CPS für die PCA beschrieben.

7 Profile von Zertifikaten und Sperrlisten
Nicht technische Sicherheitsmaßnahmen werden im CPS für die PCA beschrieben.

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 regelmäßig durchgeführt. Jährlich werden für die 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 werden können, 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 gemäß 9.3. der Policy gilt hier ebenfalls.

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

9.5 Urheberrechte

(Nichtzutreffend)

9.6 Verpflichtungen

Die PKI und die in die Registrierung eingebunden externen Stellen verpflichten sich den Bestimmungen dieser CP 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

Der Anbieter haftet unbeschränkt bei Vorsatz oder grober Fahrlässigkeit, für die Verletzung von Leben, Leib oder Gesundheit, nach den Vorschriften des Produkthaftungsgesetzes.

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.

9.9 Haftungsfreistellung

Bei der unsachgemäßen Verwendung des Zertifikats und dem zugehörigen privaten Schlüssel oder Verwendung des Schlüsselmaterials beruhend auf fälschlichen oder fehlerhaften Angaben bei der Beantragung ist die PKI von der Haftung freigestellt.

9.10 Inkrafttreten und Aufhebung

Diese CP 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 der 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 der CP werden rechtzeitig vor ihrem Inkrafttreten veröffentlicht.

9.13 Schiedsverfahren

(keine Informationen)

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 Konformität mit geltendem Recht

Es gilt deutsches Recht.

9.16 Weitere Regelungen

Die Regelungen der CP 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 dieser CP, sofern die 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