HISTORIE

Version	Stand	Bearbeiter	Änderung / Kommentar
1.00	22.12.2023	Christoph Luxem	Initiale Version

Inhalt

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 Form einer Certificate Policy (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 Datenübermittlung im Gesundheits- und Sozialwesen verständigt. Die o.g. Organisationen betreiben die PCA als gleichberechtigte Partner zur Verbesserung der Sicherheit des Datenaustausches (Anlage 16; s. Abschnitt 1.1).

Die folgenden der PCA nachgeordneten Certification Authorities (CA) werden für die Erstellung von Benutzerzertifikaten und für eine sichere Kommunikation im Gesundheitswesen und Sozialwesen genutzt:

- CA: ITSG TrustCenter für Arbeitgeber (AGV)
- CA: ITSG TrustCenter für sonstige Leistungserbringer (LE)
- CA: DKTIG TrustCenter für Krankenhäuser und Leistungserbringer PKC (DKTIG).

Einzelne in diesem Dokument beschriebene Aufgaben sind von den Certificate Authority an einen technischen Dienstleister übertragen worden. Die daraus resultierenden Verantwortlichkeiten sind in den jeweiligen Verträgen zur Einrichtung und dem Betrieb der Zertifizierungsinstanzen zwischen CA und dem Dienstleister geregelt.

Der Dienstleister führt die Zertifizierung der Request der Antragsteller durch nachdem

- Registrierung, und Authentifizierung abgeschlossen und
- die Freigabe erfolgt ist bzw. die notwendigen Daten übertragen wurden.

Die Gesamtlisten mit den gültigen Zertifikaten werden täglich erstellt, veröffentlicht und für den Download bereitgestellt.

Die hierfür verbindlichen technischen Standards sind in den „Gemeinsame Grundsätze Technik“ festgelegt. Hierbei wird insbesondere auf die Anlage 16 zur Security Schnittstelle (SECON) verwiesen „https://www.gkv-datenaustausch.de/technische_standards_1/technische_standards.jsp“.

ITSG:

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

DKTIG:

Die Schlüsselverzeichnisse für das Leistungserbringerverfahren nach §§ 301, 302 SGB V können auf der Homepage des TrustCenter der DKTIG *(Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH) h*eruntergeladen werden:

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

1.2 Gliederung des Dokumentes erfolgt nach RFC 3647

Name:	Certification Practice Statement (CP)S für das Leistungserbringer (LE) und Arbeitgeberverfahren (AGV) sowie für das Verfahren der Datenübertragung gem. § 301, 302 SGB V für den Zugang der Krankenhäuser sowie Vorsorge- und Rehabilitationseinrichtungen.
Version:	1.00
Datum:	16.12.2023
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. Die PCA signiert ausschließlich nachgelagerte fachliche „Certificate Authorities“ für die Nutzung in den Zertifizierungsstellen (siehe auch Anlage 16 Abschnitt 1.1).

Die fachlichen Zertifizierungsstellen für

- das Leistungserbringerverfahren (LE) und
- das Arbeitgeberverfahren (AGV)

werden von der ITSG Informationstechnische Servicestelle der gesetzlichen Krankenversicherung GmbH betrieben.

Die fachliche Zertifizierungsstelle für

- das Leistungserbringerverfahren für den Zugang der Krankenhäuser, Vorsorge- und Rehabilitationseinrichtungen und sonstige Leistungserbringer gem. §§301 und 302 SGB V (in diesem Dokument als Leistungserbringer oder DKTIG-Verfahren bezeichnet)

wird von der DKTIG (Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH)

betrieben.

Die genannten Zertifizierungsstellen beauftragen einen technischen Dienstleister, die Endnutzerzertifikate für die sichere Kommunikation im Gesundheits- und Sozialwesen zu erstellen.

Kontaktadressen:

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

Homepage: www.dktig.de
Montag bis Freitag von 08:30 Uhr bis 17:00 Uhr
Kontaktformular: https://dktig.de/kontakt/

Kontaktdaten: ITSG
Unter +49 (0) 6104 947 36 – 403 erreichen Sie unsere Hotline.
montags bis donnerstags von 08:30 bis 12:30 Uhr und von 13:30 bis 17:00 Uhr und freitags von 08:30 bis 14:00 Uhr.

Kontaktformular auf Homepage: https://www.itsg.de/kontakt-trust-center/

1.3.2 Registrierungsstellen (RA)

Die Registrierungsstellen überprüfen die Identität und Authentizität von Antragsstellern und Auftraggebern. Zum „Registrierungsverfahren“ und der „Identitätsüberprüfung bei Neuantrag“ die entsprechend auf andere Prüfungen der Identität angewendet werden, siehe insb. Abschnitt 3.2 im vorliegenden CPS-Dokument.

1.3.3 Zertifikatsnehmer und Zertifikatsnutzer

Zertifikatsnutzer sind Kommunikationspartner (Personen und Betriebe) die am zertifikatsbasierten Verfahren für eine sichere Kommunikation teilnehmen.

Zertifikatsnehmer sind Antragsteller die bei den oben genannten nachgeordneten Certification Authorities (siehe Abschnitt 1.3.1) End-Entity-Zertifikate zur Verschlüsselung von Verbindungen und Datentransfer im Sozialversicherungsbereich (zum Verfahren siehe Abschnitt die 1.3.1) erstellen lassen.

Die Identität und Authentizität der Ansprechpartner (auch Schlüsselverantwortliche(r) genannt) werden von den Registrierungsstellen (Abschnitt 1.3.2) der Certification Authorities überprüft.

1.3.4 Vertrauender Dritter (Relying Parties)

Vertrauende Dritte (Relying Parties) sind alle natürlichen Personen oder Organisationen, die sich auf die Vertrauenswürdigkeit der ausgestellten Zertifikate oder Signaturen verlassen.

1.3.5 Andere Teilnehmer

Mit den DV-technischen Aufgaben ist die „EVIDEN Germany GmbH, Otto-Hahn-Ring 6, 81739 München“ im folgenden Dokument „Eviden“ betraut. Im folgenden Dokument wird die Eviden „technischer Dienstleister“ genannt. Die Eviden ist im Rahmen der Ausgliederung aus der „Atos Information Technology GmbH“ entstanden.

1.4 Verwendungen von Zertifikaten

1.4.1 Erlaubte Verwendung von Zertifikaten

Die ausgestellten Zertifikate können zur Verschlüsselung von Sendungen und zur Überprüfung der Identität eines registrierten Teilnehmers genutzt werden. Die Prüfung erfolgt, anhand der den Teilnehmern der PKI-zur Verfügung gestellten Gesamtlisten und LDIF-Dateien, in denen alle gültigen Zertifikate der PKI enthalten sind.

1.4.2 Verbotene Verwendungen

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

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

Kontaktinformationen ITSG

- Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung (ITSG)
- Kostenlose Hotline
- 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-trust-center/

Kontaktinformationen DKTIG:

- Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH (DKTIG)
- Humboldtstr. 9
- 04105 Leipzig
- Tel.: 0341 / 308951 - 0
- Fax: 0341 / 308951 - 25
- Montag bis Freitag von 08:30 Uhr bis 17:00 Uhr
- E-Mail: mail@dktig.de
- Url: https://dktig.de/kontakt/

1.5.3 Prüfung der Zertifizierungsrichtlinie

Diese 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.

1.5.4 Veröffentlichung der Zertifikatsrichtlinien

Die CPS wird auf den Homepages der Zertifizierungsstellen veröffentlicht.

1.6 Definitionen und Abkürzungen

Siehe hierzu in Abschnitt 10 die verwendeten Abkürzungen.

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

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)

Die Informationen zu den öffentlichen Zertifikaten der PKI einschließlich der Gesamtlisten stehen auf der Homepage der beteiligten Zertifizierungsstellen (CA) zur Verfügung.
Die gültigen Zertifikate PCA, CA und End-Entity-Zertifikate der Arbeitgeber- und Leistungserbringerverfahren der ITSG und DKTIG werden über Gesamtlisten und LDAP-LDIF Dateien den Teilnehmern der PKI täglich zur Verfügung gestellt. Eine Aktualität der Zertifikatslisten für die Teilnehmer wird auf diesem Wege sichergestellt.

Die End-Entity-Zertifikate sind in den Gesamtlisten jeweils unter den jeweiligen Sub-CA-Zertifikaten eingeordnet, von denen bei der Erstellung signiert wurden. Die Sub-CA Zertifikate unter den jeweiligen PCA-Zertifikaten.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Die Zertifizierungsstelle der ITSG veröffentlicht die folgenden Informationen:

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

- SubCA-Zertifikate für Arbeitgeberverfahren
- Leistungserbringerverfahren
  - mit Fingerprints
  - PCA Root und CA-Zertifikate mit Fingerprint
- Sperrlisten
- LDIF-Dateien für die Nutzer eines LDAP-Directorys
- Certificate Policies und Certificate Practice Statement

Die DKTIG veröffentlicht die folgenden Informationen:

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

- SubCA-Zertifikate für
  - Leistungserbringerverfahren
  - mit Fingerprints
  - PCA Root und CA-Zertifikate mit Fingerprint
- Certificate Policies und Certificate Practice Statement

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Die gültigen Zertifikate werden als Gesamtlisten auf den Webseiten der Zertifizierungsstellen und für die Nutzer eines LDAP im Rahmen der PKI als LDIF–Dateien für eine tägliche Aktualisierung ihrer Systeme zur Verfügung gestellt.

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

ITSG

PCA CA (mit Fingerprint)	Tag des Schlüsselwechsels
DALE CA (mit Fingerprint)	Tag des Schlüsselwechsels
AGV CA (mit Fingerprint)	Tag des Schlüsselwechsels
Certificate Policies	Nach Erstellung bzw. Aktualisierung und Freigabe
Certification Practice Statement	Nach Erstellung bzw. Aktualisierung und Freigabe
Sperrlisten	Aktualisierung nach Sperrungen und turnusmäßig wöchentlich am ersten Arbeitstag
LDIF-Dateien	Tägliche LDIF-Dateien für Teilnehmer der PKI

DKTIG

PCA CA (mit Fingerprint)	Tag des Schlüsselwechsels
DKTIG CA (mit Fingerprint)	Tag des Schlüsselwechsels
CP	Nach Erstellung bzw. Aktualisierung und Freigabe
CPS	Nach Erstellung bzw. Aktualisierung und Freigabe

2.4 Zugang zu den Informationsdiensten

Die an der PKI beteiligten Nutzer und Teilnehmer erhalten täglich Zugriff auf einen aktuellen Stand aller gültigen Zertifikate. Die Gesamtlisten mit allen gültigen Zertifikaten der PKI werden täglich zusätzlich als Download auf den Webseiten der Zertifizierungsstellen zur Verfügung gestellt.

2.4.1 ITSG

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

Zertifizierungsstellen und nachgeordnete CA:

- CA: ITSG TrustCenter für Arbeitgeber (AGV)

- CA: ITSG TrustCenter für sonstige Leistungserbringer (LE)

ZERTIFIKATE MIT RSASSA-PSS-SIGNATURALGORITHMUS

- 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

2.4.1.1 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

2.4.1.2 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): 54 /(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

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

2.4.2.1 Untergeordnete CA: Organisation(o): DKTIG TrustCenter fuer Krankenhaeuser und Leistungserbringer (PKC)

(1)

- Seriennummer (dc): 83 / (hex): 53
- Gültigkeitszeitraum 30.November 2021 bis05. Januar 2027
- Signaturhashalgorithmus: SHA256
- Signaturalgorithmus: rsassaPss
- Schlüssellänge: RSA 4096 Bits
- SHA1-Fingerprint: a5a2b31b724599f999a68220a6caf58f67bae5bd

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

(2)

- Seriennummer (dc): 86 / (hex): 56
- Gültigkeitszeitraum 28. November 2023 bis 06. Januar 2029
- Signaturhashalgorithmus: SHA256
- Signaturalgorithmus: rsassaPss
- Schlüssellänge: RSA 4096 Bits
- SHA1-Fingerprint: 0c357d6962ba9cd1c77bf09f8267e3fcfafb5e99

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

2.4.2.2 Schlüsselverzeichnis der Annahmestellen und PKV

- Annahme-rsa4096.key
- PKV-rsa4096.key
- Gesamt-pkcs.key
- Gesamt-rsa4096.key

3 Identifizierung und Authentifizierung

3.1 Namen

Der Name der ausgestellten Zertifikate (Distinguished Name = DN) richtet sich nach dem Standard X.500. Der DN und die Seriennummer stellen sicher, dass keine digitalen Zertifikate für unterschiedliche Personen mit dem gleichen Namen ausgestellt werden.

3.1.1. Namensform

Mit dem Distinguished Name (DN) ist eine weltweite eindeutige Unterscheidbarkeit von Personen und Systemen gegeben. Es werden Profile für die beiden Typen von DN „allgemeine Teilnehmerzertifikate“ und „Zertifizierungsstellen (PCA und CA) unterschieden.

Folgende Felder sind nach dem X.500 Standard definiert (s.Anlage16- Abs. 4.4.4.u.4.4.5).

Zum Aufbau des DNs für Zertifizierungsstellen (PCA) s. Anlage16-Abs. 4.4.5.

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

Aufbau des DNs für Zertifizierungsstellen (CA) (s. Anlage16-Abs. 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)“

Aufbau des DN im „subject“-Datenfeld für Teilnehmerzertifikate (s. Anlage16-Abs. 4.4.5)

Pos.	Attribute		Erläuterung
1	CountryName (verpflichtend)	C	Zweistelliges Kürzel für die Länderkennung, wie „DE“ für Deutschland.
2	Organization-Name (verpflichtend)	O	Name des Trustcenters als feste Zeichenkette - „ITSG TrustCenter fuer Arbeitgeber“ - „ITSG TrustCenter fuer sonstige Leistungen“ - „DKTIG TrustCenter fuer Krankenhaeuser und Leistungserbringer (PKC)“
3	Organization-UnitName (verpflichtend)	OU	Name der Institution (Firmenname des Leistungserbringers oder des Arbeitgebers)
4	Organization-UnitName (verpflichtend)	OU	Institutionskennzeichen oder Betriebs- bzw. Zahlstellennummer. Mit vorangestellter Kennung „IK“ (bei

			Leistungserbringern) oder „BN“ (bei Arbeitgeber oder Zahlstellen).
5	CommonName (verpflichtend)	CN	Der Name einer natürlichen Person, die als Ansprechpartner für die Institution fungiert.

3.1.2 Aussagekraft der Namen

Der Name des ausgestellten Zertifikates (DN) muss den Zertifikatsnehmer eindeutig identifizieren.

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

Die Eindeutigkeit des Feldes „subject“ ist gewährleistet, um eine Feststellung des Zertifikatsinhabers ohne Verwechslungsgefahr zu ermöglichen. Der Name gibt an, wer Inhaber des Zertifikats und des damit darin enthaltenden öffentlichen und des zugehörigen privaten Schlüssels (s. Anlage 16 Abs. 4.4.5) ist.

Darüber hinaus wird jedem Zertifikat eine eindeutige Seriennummer zugeordnet, welche eine eindeutige Zuordnung zum Zertifikatsnehmer ermöglicht.

3.1.6 Anerkennung, Authentifizierung und Funktion von Warenzeichen und Markennamen

Der Antragsteller und der Zertifikatsnehmer sind für diese Überprüfungen verantwortlich.

3.2 Identitätsüberprüfung bei Neuantrag

3.2.1 Nachweis des Besitzes des privaten Schlüssels

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

3.2.2 Authentifizierung einer Organisation

Authentifiziert wird der Ansprechpartner für das Zertifikat. Die Authentifizierung einer Organisation durch die Zertifizierungsstelle ist nicht vorgesehen. Für Organisationen, die eine BN- und IK-Nummer haben, erfolgt eine Feststellung der Organisation durch die „ARGE IK“ oder die „Agentur für Arbeit“ im Rahmen der Vergabe der IK- und BN-Nummer.

3.2.3 Authentifizierung natürlicher Personen

Für die Authentifizierung natürlicher Personen werden unten angegebene Verfahren zur Prüfung der Identität herangezogen.

Zu den Verfahren gehören u.a.:

- Personalausweis
- Reisepass mit amtlicher Meldebescheinigung

- eID-Karte für Bürger der EU und des EWR
- Postident-Verfahren (ITSG für LE und AGV)
- Postident-Verfahren und zweiter Faktor (DKTIG)

3.2.4 Nicht überprüfte Zertifikatsnehmer Informationen

Es werden die Angaben zur Authentifikation und Identifikation von Zertifikatsnehmers durch das Trustcenter überprüft. BN und IK-Nummern werden anhand von Datenbank der ARGE IK und „Agentur für Arbeit“ überprüft. Andere oder zusätzliche Informationen des Zertifikatsnehmer werden nicht überprüft.

3.2.5 Prüfung der Berechtigung zur Antragsstellung

Antragsteller sind nicht nur natürliche Personen, sondern auch Organisationen und Rechtsformen des öffentlichen und privaten Rechts.
Bei der DKTIG sind Antragsteller die Institutionen/Organisationen, mit denen ein TrustCenter-Vertrag besteht. Der Antragsteller beauftragt einen Ansprechpartner (Schlüsselverantwortlichen) den Antrag für ein Zertifikat bei der DKTIG zu stellen.

Die Autorisierung einer natürlichen Person als Handlungsberechtigter im Namen einer Organisation erfolgt organisationsintern nach einem dafür geeigneten und vorgesehenen Verfahren.

Für die teilnehmenden Organisationen müssen bereits IK – (Institutionskennzeichen) oder BN - (Betriebsnummer) Nummer vorliegen als Voraussetzung für die Beteiligung an der PKI.

Die Prüfung der Organisation und Vergabe der IK - und BN – Nummer erfolgt in gesonderten vorgelagerten Verfahren bei der „ARGE IK“ und der „Agentur für Arbeit“ (siehe Abschnitt 3.2.2) entsprechend den Verfahren den referenzierten Rechtsgrundlagen nach dem Sozialgesetzbuch.

- Betriebsnummer (§ 18i ff. SGB IV)

Die Betriebsnummer wird von der Agentur für Arbeit vergeben.
(https://www.arbeitsagentur.de/unternehmen/betriebsnummern-service)

- Rechtsgrundlage für die Betriebsnummer

Die Betriebsnummer ist normiert in den Paragrafen 18i bis 18n, Viertes Buch Sozialgesetzbuch (SGB IV).

- Institutionskennzeichen (§ 293 SGB V)

Das Institutionskennzeichen wird von der ARGE IK vergeben.
(https://www.dguv.de/arge-ik/index.jsp)

- Rechtsgrundlage für das Institutionskennzeichen:

Fünftes Buch Sozialgesetzbuch (SGB V) § 293 - Kennzeichen für Leistungsträger und Leistungserbringer

3.2.6 Kriterien für Cross-Zertifizierung und Interoperabilität

(Nichtzutreffend). Eine Cross-Zertifizierung ist nicht geplant.

3.3 Identifizierung und Authentifizierung

3.3.1 Routinemäßige Zertifikatsbeantragung mittels Folgeantrag

3.3.1.1 Zertifikatsbeantragung

Die Identifizierung und Authentifizierung für eine Zertifikatsneubeantragung erfolgt entsprechend dem initialen Antragsprozess.

Die Identifizierung und Authentifizierung der Antragsteller und Schlüsselverantwortlichen und damit der Nachweis der Identität erfolgt durch eine geeignete Maßnahme (siehe hierzu 5.5 Anlage 16), die die Anforderungen an eine substanzielle Authentifizierung erfüllt. Die Registration Authority (im Folgenden R.A.) muss sich in geeigneter Form überzeugen, dass der Antragsteller tatsächlich derjenige ist, der er zu sein vorgibt.

Die aktuell hierfür verwendeten Maßnahmen finden Sie auf den Webseiten der Trustcenter ITSG und DKTIG.

3.3.1.2 Folgeantrag für das Leistungserbringer-Verfahren und das Arbeitgeberverfahren (AGV)

Ein Sonderfall der Identifizierung und Authentifizierung ist hierbei bei papierlosen Online-Folgeantrag zu berücksichtigen. Der Online-Folgeantrag muss mit einem gültigen Zertifikat vom ITSG-TrustCenter elektronisch signiert werden. Der Online-Folgeantrag darf nur durch den identifizierten Antragsteller gestellt werden. In anderen Fällen ist eine Erstantrag notwendig.

Auf neue Identifizierung und Authentifizierung kann aber nur verzichtet werden, wenn sich neben den Antragsdaten nicht der Ansprechpartner geändert hat.

Hinsichtlich der Einzelheiten der aktuell genutzten Identifizierung- und Authentifizierung-Verfahren für Antragsteller und Schlüsselverantwortliche wird auf die Webseiten der Zertifizierungsstellen unter *Abschnitt 1.3.1* verwiesen.

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. Suspendierung oder eine temporäre Sperrung sind nicht vorgesehen.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Nur autorisierte und berechtigte Personen und Institutionen können die Sperrung eines Zertifikates veranlassen.

Die Authentisierung für den Antrag zur Durchführung der Sperrung hat in einer geeigneten Art und Weise zu erfolgen (siehe oben Abschnitt 3.2.3.).

Die Identität des Antragsstellers bei Sperranträgen wird dokumentiert. Der Zertifikatsnehmer wird über die Sperrung des Zertifikates unterrichtet.

Der Antrag ist auf seine Korrektheit zu prüfen. Es ist auch die Berechtigung des Antragstellers zu prüfen den Sperrantrag zu stellen. Die Unterschrift des autorisierten Ansprechpartners kann durch die seines Vorgesetzten ersetzt werden.

4. Betriebliche Anforderungen im Lebenszyklus von Zertifikaten

4.1 Zertifikatsantrag

4.1.1 Zertifikatsanträge können von den Zertifikatsnutzern nach Abschnitt 1.3.3 gestellt werden.

Der Antragsprozess für Zertifikate findet bei einer Erstbeauftragung entsprechend den Voraussetzungen für einen Antrag nach Abschnitt 3.2 statt.

4.1.2 Registrierungsprozess und Zuständigkeit

Die Beantragung von Zertifikaten erfolgt im Rahmen eines mehrstufigen Registrierungsprozesses. Folgende Prüfungen werden durchgeführt:

- Prüfung der Berechtigung des Antragstellers bzw. des Ansprechpartners
- Vollständigkeit und Korrektheit des Antrags
- Eindeutigkeit des DN
- Übereinstimmung der Antragsdaten und der Daten im Request
- Technische Prüfung des Request inkl. Hashwert / Fingerprint
- Prüfung der Authentizität

Neben der inhaltlichen Prüfung wird festgestellt, ob alle erforderlichen Antragskomponenten übermittelt wurden.

4.1.3 Zertifikatsanträge

Der Zertifikatsantrag für Endnutzerzertifikate in den Leistungserbringerverfahren und Arbeitgeberverfahren besteht ausfolgenden Daten:

4.1.3.1 Verfahren LE und AGV der ITSG

- BN, gesonderte Absendernummer, Zahlstellennummer, Hochschulnummer, IK
- Name des Antragstellers (Firma / Institution)
- Name des Ansprechpartners des Antragsstellers
- Telefon und E-Mail-Adresse des Ansprechpartners
- Hausanschrift des Antragsstellers
- optionale Rechnungsanschrift
- Requestdatei für Zertifizierung (PKCS#7)
- Unterschrift des Ansprechpartners

List der vollständigen Antragsunterlagen:

- siehe: https://www.itsg.de/produkte/trust-center/zertifikat-beantragen/
- Registrierungsportal der ITSG (https://registrierungsportal.itsg.de/regportal/client/de/login)
- sowie dem von Ihnen genutzten elektronischen Programm für die Antragsstellung.

4.1.3.2 Verfahren der DKTIG

- Name der Institution/Organisation
- Adresse der Institution/Organisation
- Institutionskennzeichen
- Name des Ansprechpartners (Schlüsselverantwortlicher); dieser wird vom Vertretungsberechtigten der Organisation benannt

- Unterschrift des Vertretungsberechtigten auf dem Antrag „Ernennung zum Schlüsselverantwortlichen“
- Kontaktdaten des Ansprechpartners (Schlüsselverantwortlichen)
    - Vor- und Nachname(n)
    - Geburtsdatum
    - Telefonnummer
    - E-Mail (personalisiert)
    - Unterschrift des Ansprechpartners auf dem Fingerprint
- Requestdatei für Zertifizierung (PKCS#7)
- Datenschutzeinwilligung

Informationen zum vollständigen Zertifikatsantragsverfahren:
https://dktig.de/zertifizierungsablauf/

4.2 Bearbeitung von Zertifikatsanträgen

4.2.1 Durchführung der Identifikation und Authentifizierung

Der Antragsteller bzw. Ansprechpartner muss die Antragsinformationen zur Verfügung stellen, die als Voraussetzung für eine Zertifikatserstellung in Abschnitt 4.1.3 aufgeführt werden.

Die Identifikation und Authentifizierung von Zertifikatsnehmern werden gemäß den Anforderungen nach Abschnitt 3.2 (Identitätsprüfung bei Neuantrag) durchgeführt.

4.2.2 Annahme und Ablehnung von Zertifikatsanträgen

Es besteht keine vertragliche Verpflichtung oder Anspruch auf die Erteilung eines Zertifikates ohne abgeschlossene Prüfung.

4.2.3 Bearbeitungsdauer von Zertifikatsanträgen

Die Bearbeitungsdauer von vollständig eingegangenen Zertifikatsanträgen bis zur Veröffentlichung kann bis zu sieben Tage betragen.

Übersicht über Auftragsstatus der Aufträge in den vorgenannten Verfahren beim Dienstleiter

Status	**Bedeutung**
Registrierung	Registrierung und Authentifizierung der Identität der Ansprechpartner für die - Leistungserbringer-Verfahren für ITSG und DKTIG und - dem Arbeitgeberverfahren (AGV). Nach Abschluss der Registrierung wird der Auftrag zur Zertifizierung weitergeleitet. Der Status der Zertifizierung ist für alle Verfahren (LE, AGV, i. V. m. § § 301,302 SGB V) gleich.
Status des Zertifizierungsauftrags	

Status	Bedeutung
• neu	Der Antrag ist zur Zertifizierung übertragen worden und wurde noch nicht bearbeitet.
• vollständig	Die Prüfung des Antrages wurde erfolgreich durchgeführt und ist positiv abgeschlossen worden: ***Auftrage mit dem Status "vollständig“ werden bei der nächsten Zertifizierung verarbeitet.*** Die Prüfung und der Vergleich der Daten des Request und der Antragsdaten wurde durchgeführt sowie die - Visuelle und - technische Prüfung wurde abgeschlossen.
• vorbearbeitet	Der Antrag ist vorbearbeitet und bereit für die Zertifizierung. Die Prüfung der Antragdaten und technischen Voraussetzungen ist inklusive der visuellen Prüfungen erfolgt.
• Pro exportiert	Der digitale Request, der *Prototyp*, zum Antrag wurde zur Zertifizierung auf einen Datenträger exportiert. Mit dem Datenträger wird die Zertifizierung in einem Offline-System durchgeführt.
• CRP importiert	Das Ergebnis der Zertifizierung, die *Zertifikatsantwort*, wurde nach der Offline-Zertifizierung an dem CA-System wieder in die Verwaltungsanwendung importiert.
• nachbearbeitet	Antrag und erstelltes Zertifikat wurde validiert / nachbearbeitet. Das Ergebnis der Zertifikatserstellung wird überprüft. Das Zertifikat ist bereit zur Bereitstellung und Veröffentlichung.
• Veröffentlichung und • Bereitstellung	- Bereitstellung bedeutet das Zertifikat wird dem Antragsteller zur Verfügung gestellt. - Veröffentlichung bedeutet -dass das Zertifikat mit den Gesamtlisten allen PKI-Teilnehmer zur Nutzung zur Verfügung gestellt wird.
• fehlerhaft	Der Antrag ist fehlerhaft. Der Antragsstellt wird über den Fehler unterrichtet.

4.2.4 Bearbeitung Zertifikatsanträge der Verfahren LE, AGV und Datenaustausch n. §§301,302 SGB V

4.2.5 Registrierung und Identifizierung in den Verfahren

Die Identifizierung für den Zertifikatsantragsprozess findet entsprechend den Voraussetzungen nach Abschnitt 3.2 statt.

ITSG

Die Antragsteller registrieren sich über das Portal der ITSG für die *Verfahren LE und AGV*. Die Antragsteller werden über ein externes Post-Ident-Verfahren identifiziert. Dieser Identifizierungsprozess über das Post-Ident-Verfahren löst alle anderen derzeit genutzten Identifizierungsverfahren für die Verfahren „LE“ und „AGV“ der ITSG ab.

Siehe hierzu die Details zum Registrierungsverfahren https://www.itsg.de/produkte/trust-center/zertifikat-beantragen/ .

DKTIG

Für das *Leistungserbringer-Verfahren der DKTIG* erfolgt eine Registrierung über das Serviceportal der DKTIG unter: www.dktig-serviceportal.de
Die Ansprechpartner werden über ein externes Post-Ident-Verfahren identifiziert. Zusätzlich wird die Registrierung am Serviceportal durch einen zweiten Faktor abgesichert.

Siehe hierzu die Details zum Registrierungsverfahren https://dktig.de/dktig-serviceportal/

4.2.5.1 Überprüfung der Betriebsnummer und Institutionskennzeichen:

- Die Betriebsnummern und Institutionskennzeichen werden mit aktuellen Daten überprüft, um die Adresse des Betriebs oder Intuition für das Antragsverfahren zu verifizieren.
- Die BN-Nummer dient als Identifikationsmerkmal für die Beschäftigungsbetriebe und wird von der Bundesagentur für Arbeit (BA) §§ 18i-18m SGB IV vergeben
- Überprüfung des eindeutigen Institutionskennzeichen (IK) der ARGE-IK nach § 293 SGB V.

Im Fall – das die Adressunterlagen nicht mit den Adressdaten bei ARGE IK, Bundesagentur für Arbeit (BA), dem Handelsregistereintrag oder dem Eintrag im InEK-Standortverzeichnis gem. § 293 Abs.6 SGB V übereinstimmen, muss eine Korrektur der Adresse durch den Antragssteller bzw. den Ansprechpartnervorgenommen werden.

4.2.5.2 Übersicht über die Zertifikatsanträge in den Verfahren:

- *OSTC-Folgeanträge der ITSG (s. Abschnitt 3.3.1.2 zu Folgeanträgen)*.
  Die Antragsart „Folgeantrag“ ist möglich, wenn der Antrag mit einem gültigen Zertifikat des Antragstellers gestellt wird und keine Änderungen im Inhalt des Zertifikats und bei den Ansprechpartnern seit der letzten Identifizierung erfolgt sind. Sind die Voraussetzungen nicht gegeben - so ist eine neue Registrierung über das Registrierungsprotal notwendig.

- OSTC-Erstanträge (ITSG) sind rein digitaler Antrag über die OSTC-Schnittstelle. Der Antragsteller stellt den Antrag und schickt den Request über dieselbe Schnittstelle. Eine Registrierung und Identifizierung erfolgt über das Registrierungsportal.

- DKTIG-Verfahren -

  Die Registrierung der Schlüsselverantwortlichen der beteiligten Einrichtungen für das Verschlüsselungsverfahren, erfolgt über das Serviceportal der DKTIG (https://dktig-serviceportal.de/ insb. 3.2.3 Authentifizierung natürlicher Personen). Nur registrierte Schlüsselverantwortliche können im Serviceportal Erst- und Folgeanträge stellen.

4.2.5.3 Erstellung der Zertifizierung und Antragsprüfung beim technischen Dienstleister

Nach dem Abschluss der Registrierung in den Verfahren LE, AGV der ITSG und dem Leistungserbringerverfahren der DKTIG wird ein Prüfungs- *und Zertifizierungsauftrag* an den technischen Dienstleister geschickt.

4.2.5.4 Antragsinhalt

Zu einem (vollständigen) Antrag gehört immer neben den Antragsdaten eine s.g. *elektronische Zertifikatsanforderung* oder auch *Request-Datei (CRQ)*, die u.U. auf einem anderen Weg wie

- Upload-Portal,
- OSTC eingeht.

Die zum Antrag gehörige Daten werden vom Antragsteller in den Registrierungsportalen der ITSG und DKTIG eingegeben und nach Durchführung der Authentifizierung und Freigabe von der ITSG über die Rest-API Schnittstelle und von der DKTIG mittels verschlüsselter E-Mail-Kommunikation zum technischen Dienstleister übertragen, von dem die Zertifizierung durchgeführt wird.

4.2.5.5 Prüfung der Anträge

Vom technischen Dienstleister werden vor der Zertifizierung die Erfüllung der Anforderungen ebenfalls nochmal kontrolliert:

- Die Prüfung erfolgt bei der ITSG gegen die Antragsdaten aus dem Registrierungsportal. Es werden Antragsdaten und Daten im Request durch einen Mitarbeiter oder Mitarbeiterin geprüft (siehe hierzu folgenden Abschnitt „Prüf- und Zertifizierungsauftrag“).
- Bei Anträgen der DKTIG werden die übermittelten Antragsdaten, der Request und der Fingerprint geprüft.
- Daneben wird auch die Erfüllung der technischen Vorgaben für den Request aus Anlage 16 als Voraussetzung für das Erstellen des neuen Zertifikats über automatische Prüfungen verifiziert.

In der Anwendung wird der aktuelle Bearbeitungsstatus der Zertifikatsanträge verwaltet und dokumentiert.

4.2.5.6 Prüf- und Zertifizierungsauftrag

Der Dienstleister führt im Detail nach der Übertragung an ihn die folgenden Prüfungen durch, um den Antragsstatus „vorbearbeitet“ als Voraussetzung für eine Zertifizierung zu setzten:

- Überprüfung, ob alle erforderlichen Antragskomponenten des Antragstellers an den technischen Dienstleister (Request) und von der Registrierungsstelle an ATOS übermittelt wurden.
- Eindeutigkeit des DN
- Eine visuelle Überprüfung, ob die Antragsdaten des Antragstellers korrekt sind.
- Visuelle Überprüfung, ob Antragsdaten des Antragstellers mit dem Request überein-stimmen.
- Letzte visuelle Überprüfung, ob Request für Zertifizierung technisch korrekt ist.
- Visuelle Überprüfung, ob Hashwert des Request richtig ist.

- Wenn Antragskomponenten nicht korrekt oder unvollständig sind, wird eine Fehlermeldung in der Onlineantragsverfolgung verfasst.
- Technische Prüfung des Request inkl. Hashwert / Fingerprint, ob der Request Anforderungen aus der Anlage 16 entspricht

4.3 Ausstellung von Zertifikaten

4.3.1 Tätigkeiten der Ausstellung von Zertifikaten

Die Ausstellung von Endnutzerzertifikaten unterliegt festgelegten Prüfungen und wird dokumentiert und auch durch die Systeme protokolliert.

Die Zertifikatserstellung gliedert sich in drei Abschnitte:

- dem Export der vorbearbeiteten Anträge **aus** dem Verarbeitungssystem,
- der Zertifizierung am Offline CA-System und
- den anschließenden Import der erstellten Zertifikate **in** das Verarbeitungssystem und die Bereitstellung des Zertifikats für den Antragsteller bzw. den Ansprechpartner sowie die Veröffentlichung des Zertifikats für die PKI.

Die exportierten Request-Dateien aus der Applikation werden Prototypen oder auch Prototyp-Dateien genannt.

Inhaltlich handelt es sich um die ursprüngliche Request-Datei, ergänzt um eine Zeile (am Anfang der Datei) mit Meta-Informationen wie bspw. dem zu setzenden Gültigkeitszeitraum.

Alle Anträge, die sich im Status „vorbearbeitet“ befanden und deren Request-Dateien zur Zertifizierung auf einen Datenträger exportiert wurden, erhalten während des Exports automatisch den Status „exportiert“.

4.3.1.1 Durchführung der Zertifizierung in einer gesicherten Umgebung

Die eigentliche Zertifikatserstellung wird von und bei dem technischen der Dienstleister der Certificate Authority durchgeführt.
Der Zertifizierungsprozess am CA-System für alle genannten Verfahren erfolgt in einem gesonderten Sicherheitsbereich an Offline-Systemen beim technischen Dienstleister.

Der Datenträger mit den exportierten Prototyp-Dateien wird in die gesicherte Umgebung mitgenommen, um dort am Offline-CA-System die Signierung und Zertifikatserstellung durchzuführen. Nach der Anmeldung am CA-System wird der Zertifizierungsvorgang vom Bearbeiter durch einen entsprechenden Skriptaufruf gestartet.

Die Ausgaben werden vom Bearbeiter geprüft. Genauere Information zu Verwendung des Skriptes, sowie möglicher Fehlermeldungen und der entsprechende Umgang mit diesen bzw. deren Behebung sind im Betriebskonzept zum CA-System dokumentiert.

Nachdem das Skript erfolgreich beendet wurde und die Seriennummern in den Logbüchern dokumentiert wurden, meldet sich der Bearbeiter vom CA-System ab und entfernt den Datenträger wieder, der nun die Ergebnisse der Zertifizierung enthält, und verlässt mit diesem die gesicherte Umgebung, um die erzeugten Dateien im nächsten Schritt in die Anwendung zu importieren. Sperrungen können in der Sicherheitsumgebung ggf. ebenfalls durchgeführt werden

Nach der Erstellung und Import in die Zertifikatsverwaltung werden die Zertifikate in der weiteren Bearbeitung nochmal abschließend mit dem Antrags- und den Authentifizierungsunterlagen verglichen.

4.3.1.2 Rollen für die Zertifizierung

Die Zertifizierungstätigkeit besitzt eine eigene Rolle. Mit dieser Rolle werden nur Zertifizierungen durch Mitarbeiter durchgeführt. Diese Rolle besitzt nicht die Berechtigungen eines Key-Managers.

Administrative Tätigkeiten (Schlüsselerzeugung, -backup und Löschung von Schlüsselpaaren) am Hardware Sicherheitsmodule (HSM) werden dagegen nur im Rahmen von Schlüsselzeremonien unter gleichzeitiger Anwesenheit von zwei Key-Manager des technischen Dienstleisters nach dem Vier-Augenprinzip durchgeführt.

Die Vergabe der Rollen für Zertifizierung und u.a. Key-Manager Rolle wird über Rollenkonzepte, Rollenzuweisung und Freigabe abgesichert. Für die Schlüsselzeremonie werden die Vorgaben der TR3145-1 eingehalten. Siehe hierzu auch Abschnitt 5.2.1 „Vertrauenswürdige Rollen“.

4.3.2 Erstellung, Benachrichtigung, Bereitstellung und Veröffentlichung der Zertifikate

Die Antragsteller bzw. Ansprechpartner werden über die Erstellung und Bereitstellung der beantragten Zertifikate benachrichtigt. Die Bereitstellung des Zertifikates erfolgt entsprechend dem von ihm gewählten Antragsweg. Abhängig von der Zertifizierungsstelle stehen u.a. folgende Bereitstellungen zur Verfügung:

- Das Zertifikat kann über die Online-Antragsverfolgung vom jeweiligen Antragsteller bzw. Ansprechpartner heruntergeladen werden
- Das Zertifikat kann von jedem Verfahrensteilnehmer über den Mail-Responder abgerufen werden
- Das Zertifikat kann von jedem Verfahrensteilnehmer der ITSG zusätzlich über die OSTC-Schnittstelle abgerufen werden
- Versand des Zertifikates an die E-Mail-Adresse des Request Absenders (auch Dienstleister) vor.

Gleichzeitig mit der Bereitstellung des Zertifikates an den Antragsteller, erfolgt (in der Regel) auch die Bekanntmachung des Zertifikats im jeweiligen Verfahren. Dazu wird dieses einerseits im s.g. *Zertifikatsarchiv* zum Abruf über den Mail-Responder und die OSTC-Schnittstelle abgelegt, andererseits wird es in die *Gesamtliste* des jeweiligen Verfahrens aufgenommen.

Bei der *Gesamtliste* handelt es sich um die Liste der jeweils zuletzt ausgestellten, gültigen Zertifikate aller Teilnehmer des jeweiligen Verfahrens. Sie wird von den Verfahrensteilnehmern als *White List* (neben den Sperrlisten im Sinne einer *Blacklist*) verwendet, um die Zertifikate der jeweiligen Gegenstelle zu ermitteln, die dann zur Signaturvalidierung und -Verschlüsselung herangezogen werden.

Die Gesamtlisten (sowie weitere Sammellisten) werden in der Anwendung verwaltet. Die Erstellung und Veröffentlichung bzw. Bekanntmachung der neuen und aktualisierten Liste erfolgt aus der Anwendung heraus.

Die Zertifikate werden durch die Verteilung der Gesamtlisten und Lieferungen für den LDAP täglich veröffentlicht und aktuell an die Teilnehmer der PKI verteilt oder bereitgestellt.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme des Zertifikats

Die Annahme des Zertifikats kann konkludent durch die Nutzung des Zertifikats erfolgen, ohne dass es eine Erklärung gegenüber dem TrustCenter erfordert.

4.4.2 Veröffentlichung des Zertifikates durch die CA

Die Zertifikate werden auf den Seiten der beteiligten Zertifizierungsstellen veröffentlicht. Eine Veröffentlichung der Zertifikate für einen Verzeichnisdienst erfolgt mittels LDIF-Dateien (ITSG) und Gesamtlisten für die Teilnehmer der PKI. Siehe hierzu bereits Abschnitt 2.4 „Zugang zu Informationsdiensten“.

4.4.3 Benachrichtigung weiterer Instanzen durch die CA

(Nichtzutreffend)

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Nutzung des privaten Schlüssels

Die Nutzung des privaten Schlüssels darf ausschließlich durch den Zertifikatsnehmer möglich sein. Er hat für die Sicherheit des privaten Schlüssels zu sorgen.

Der Zertifikatsnehmer hat insbesondere auch die Pflicht

- unverzüglich der CA anzuzeigen, wenn die Angaben in dem ausgestellten Zertifikat nicht oder nicht mehr den Tatsachen entsprechen
- die Regelungen der CA für die Sicherheit, Speicherung und Nutzung der privaten Schlüssel und der erstellten Zertifikate zu beachten
- die Beschränkungen im Hinblick auf die Verwendung des privaten Schlüssels einzuhalten (siehe Abschnitt 1.4.1)
- die Sperrung der Zertifikate unverzüglich bei einer Kompromittierung des privaten Schlüssels zu veranlassen.

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 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 Zertifikatsauftraggebers
(Nichtzutreffend)

4.6.5 Es gelten die Regelungen gemäß Abschnitt 4.4 zur *Zertifikatsakzeptanz*
(Nichtzutreffend)

4.6.6 Es gelten die Regelungen zur *Veröffentlichung* gemäß Abschnitt 4.4.2
(Nichtzutreffend)

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 Schlüsselpaar generiert. Es erfolgt hierbei eine Überprüfung der Aktualität der genutzten Schlüsseldaten und eine Anpassung der Schlüssel- und Zertifikatsdaten (siehe Abschnitt 4.8).

4.8 Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung
Eine Zertifikatserneuerung erfolgt nur mit einem neuen Schlüsselpaar. Im Rahmen der Zertifikatserneuerung werden die Zertifikatsinhalte und die verwendeten technischen Parameter überprüft und aktualisiert.

4.8.1 Zertifikatserneuerung mit Schlüsselwechsel und Anpassung von Daten und technischen Parametern.

Eine Zertifikatserneuerung ist notwendig bei:

- Ablauf der Nutzungszeit der CA und untergeordneten Zertifikatsstellenzertifikate aufgrund des Schalenmodells
- Ablauf der Gültigkeit des Zertifikats (EE-Zertifikate)
- Neubeantragung nach einer Sperrung des letzten Zertifikates
- Änderung in den Daten des bisherigen Zertifikates
- Änderungen bzw. Aktualisierungen von technischen Parametern wie Algorithmen, Schlüssellänge, Signaturalgorithmen und der Gültigkeitsdauer des Zertifikats, wenn eine Sicherheit ohne eine Anpassung der Zertifikatsinhalte gewährleistet ist.

4.8.2 Planung und Beantragung eines Schlüsselwechsels
Der turnusmäßig vorgesehene Schlüsselwechsel ergibt sich aus der festgelegten Laufzeit der PCA, die der untergeordneten Zertifizierungsstellenzertifikaten sowie deren festgelegte Nutzungs- und Gültigkeitsdauern aufgrund des verwendeten Schalenmodells.

Daneben kann eine außerplanmäßige Zertifikatserneuerung von den Zertifikatsnehmern aus technischen oder sicherheitstechnischen Gründen notwendig sein oder beantragt werden.

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

4.8.3 Ablauf der Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Der Prozess der Zertifikatserneuerung wird entsprechend dem Verfahren der erstmaligen Antragstellung durchgeführt. Die Erneuerung des Schlüsselpaars sowie die Erzeugung des Zertifikats wird in einem Sicherheitsbereich im Vier-Augen-Prinzip durchgeführt.

4.8.4 Benachrichtigung des Zertifikatsnehmer

Angewendet werden die initialen Regelungen für die Zertifikatserstellung entsprechend. Der Zertifikatsnehmer wird über die Erstellung des Zertifikates informiert. Eingehalten müssen die Anforderungen an einen sicheren Datenaustausch mit dem Zertifikatsnehmer.

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 aus.

4.8.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle

Die neuen Zertifikate werden in den Gesamtlisten täglich hinzugefügt und veröffentlicht. Insoweit wird auf die initialen Regelungen für die Zertifikatserstellung (s. Abschnitte 4.4, 4.6) verwiesen.

4.8.7 Benachrichtigung weiterer Instanzen über die Zertifikatserstellung

(Nichtzutreffend)

4.9 Sperrung von Zertifikaten

Die Voraussetzung, Gründe und der Ablauf der Sperrung von Zertifikaten müssen beschrieben werden.

Bei den Verfahren des TrustCenters handelt es sich um s.g. *Whiteliste*-Verfahren, d.h. alle gültigen Zertifikate werden nach Verfahren in der Liste täglich neu veröffentlicht und an die Teilnehmer der PKI verteilt. Nur Zertifikate dieser Liste dürfen als gültig betrachtet werden und zur Validierung einer Signatur oder Verschlüsselung von Inhalten herangezogen werden. Die Liste enthält dabei alle relevanten PCA- und CA-Zertifikate sowie das jeweils zuletzt ausgestellte, noch gültige Zertifikat aller Verfahrensteilnehmer. Eine Sperrliste – als *blacklist* – ist demnach nicht erforderlich.

In den anhängigen Verfahren werden auch Sperrungen durchgeführt und entspr. Sperrlisten erzeugt und verwaltet.

Durchzuführende Sperrungen gehen in der Regel mit einer s.g. *Sperrdatei* ein. Im Rahmen des Exports der Prototyp-Dateien für die Zertifikatserstellung werden die Sperraufträge mittels Datenträger auf das Offline–CA-System übertragen und dort die Sperrung durchgeführt.

Im letzten Schritt eines jeden Zertifizierungsvorganges in der Sicherheitsumgebung wird eine neue Sperrliste je Verfahren erzeugt. Dies geschieht unabhängig davon, ob in dem jeweiligen Zertifizierungslauf eine (neue) Sperrungen vorgenommen oder Zertifikate ausgestellt wurden.

Die erzeugten Sperrlisten werden gemeinsam mit den erstellten Zertifikaten im Rahmen des Zertifizierungsvorgangs auf einem Datenträger in die CA – Anwendung zu weiterer Verarbeitung importiert. Von dort aus werden sie im Rahmen der Veröffentlichung auf weiteren Systemen abgelegt und verteilt bzw. stehen dort zum Abruf bereit. Siehe zur Authentifizierung der Sperrung Abschnitt (3.4.).

4.9.1 Gründe für die Sperrung

Ein Benutzerzertifikat muss gesperrt werden, wenn nachfolgende Gründe vorliegen:

- Der ursprüngliche Zertifikatsrequest war nicht autorisiert und wurde auch nicht rückwirkend autorisiert.
- Es liegen Beweise vor, dass der private Schlüssel des Zertifikats kompromittiert wurde.
- Es liegen Beweise vor, dass das Zertifikat missbräuchlich eingesetzt wurde.
- Der Zertifikatsnehmer hält wesentliche Verpflichtungen nach der CP oder dem CPS (z.B. für die Sicherheit seines privaten Schlüssels) nicht ein.
- Die Informationen und Angaben im Zertifikat sind nicht korrekt oder missverständlich.
- 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 oder Sub-CA hat den Verdacht, dass der eigene private Schlüssel kompromittiert wurde. In diesem Fall werden sämtliche betroffenen bzw. ausgestellten Zertifikate gesperrt.
- Richterliche Urteile oder eine Weisung einer die Aufsicht führenden Behörde liegt vor.
- Die Schlüssellänge, Gültigkeitsdauer oder die benutzen Algorithmen gewährleisten keine ausreichende Sicherheit mehr. In diesem Fall werden die Zertifikate durch die PKI gesperrt.

4.9.2 Berechtigung eine Sperrung zu beantragen

Die Sperrung kann beantragt werden durch den Zertifikatsnehmer oder einem von Ihm Beauftragten. Der Zertifikatsnehmer kann nur die Sperrung seines eigenen Zertifikates beantragen (siehe auch 3.4 i.V.m. mit Abschnitt 3.2.3).

4.9.3 Ablauf einer Sperrung

Die Sperrung eines Zertifikates muss schriftlich beantragt werden.

Die PKI muss Sperrungsmöglichkeiten, für die in 4.9.2 genannten Beteiligten bereitstellen und auf Problemreports reagieren. Die PKI führt die Sperrungen durch und veröffentlicht die Sperrliste.

4.9.4 Fristen für den Zertifikatsnehmer und Auftraggeber

Beim Vorliegen eines Sperrgrundes nach Abschnitt 4.9.1 muss die Sperrung des Zertifikates unverzüglich 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 gegebenenfalls die Ergebnisse der Bewertung zu besprechen und zu entscheiden, ob eine Zertifikatssperrung notwendig ist.

Einfluss auf die Bewertung und die Dringlichkeit der Entscheidung über eine Sperrung haben:

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

Im Zuge der Sperrung muss die sperrende CA abhängig von der möglichen Höhe des Risikos, dem Schadens- und den Auswirkungen einen Bericht oder eine Zusammenfassung erstellen.

4.9.6 Sperrprüfungen durch Zertifikatsnutzer und Relying Parties

Die PKI stellt über das tägliche Erzeugung und Verteilung von Gesamtlisten sicher, dass nur gültige Zertifikate für die Nutzer der PKI -Teilnehmer bereitstehen.

Die PKI beruht auf einem Whitelist-Verfahren. Die Gesamtlisten enthalten jeweils alle gültigen PCA-, Sub-CA und Benutzerzertifikate. Daneben werden zusätzlich Sperrlisten erstellt und zusammen mit den Gesamtlisten an die Teilnehmer der PKI verteilt.

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Sperrlisten werden werktäglich neu erzeugt.

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 in den werktäglich neu erstellten Gesamtlisten nur gültige Zertifikate.

Gesperrte Zertifikate sind in den entsprechenden Sperrlisten zu finden.

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 CA-Zertifikat auch alle von ihren ausgestellten Zertifikaten gesperrt. Abschnitt 4.9.5 wird für die Bewertung und den Umfang der notwendigen Sperrungen angewendet. Bei der Komprimierung eines privaten Schlüssels eines Zertifikatsnehmers (End-Entity Zertifikat) wird nur das dazugehörige Zertifikat unverzüglich gesperrt.

4.9.13 Gründe für eine Suspendierung

Bei Vorliegen von Sperrgründen werden Zertifikate unwiderruflich gesperrt und nicht suspendiert. Eine temporäre Sperrung wird in der PKI nicht genutzt.

4.9.14 Beantragung einer Suspendierung
(Nichtzutreffend)

4.9.15 Ablauf einer Suspendierung
(Nichtzutreffend)

4.9.16 Dauer einer Suspendierung
(Nichtzutreffend)

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)
Onlinesperrung und eine online Statusprüfung für Zertifikate stehen derzeit nicht zur Verfügung. Die PKI basiert auf dem Whitelist-Verfahren. Die gültigen Zertifikate werden über die Gesamtlisten und LDIF–Dateien täglich den PKI-Teilnehmern täglich 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 Schlüsselwiederherstellung
(Nichtzutreffend) Schlüsselhinterlegung wird nicht angeboten.

5 Nicht technische Sicherheitsmaßnahmen
Die Certificate Authorities (CA) bzw. der technische Dienstleister müssen vor ihrer Betriebsaufnahme ein ISMS (Information Security Management System) einführen.

Die im Folgenden beschriebenen Sicherheitsmaßnahmen werden durch den technischen Dienstleister abgesichert und erfüllt.

Die umgesetzten Sicherheitsmaßnahmen sind für das TrustCenter in einem (nicht öffentlichen) Sicherheitskonzept mit Anlagen und in Standortkonzepten zusammengefasst.

Das Sicherheitskonzept muss berücksichtigen:

- administrative, organisatorische, technische und infrastrukturelle Sicherungsmaßnahmen, 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
- eine Risikobewertung, die internen und externen Bedrohungen aufführt, die zu unautorisierten Zugriffen, Veröffentlichungen, Missbrauch, Austausch oder Zerstörung von Zertifikatsdaten oder des Zertifikatsmanagement-Prozesses führen können
- die physikalische Sicherheit und umweltbezogene Maßnahmen
- Systemintegritätsmaßnahmen, Konfigurationsmanagement, Erhaltung der Integrität von vertrauenswürdigem Code, Malware-Erkennung und Vorsichtsmaßnahmen
- das Benutzermanagement, eine eigene Vergabe von vertrauenswürdigen Rollen, Ausbildung, Sensibilisierung und Fortbildung.

Im Rahmen der notwendigen Risikobewertung müssen ebenfalls Eintrittswahrscheinlichkeit und der möglicherweise eintretende Schaden im Sicherheitskonzept bewertet werden. Die Einhaltung der generellen Sicherheitsanforderungen durch den technischen Dienstleister wird durch eine Zertifizierung nach ISO 27001 nachgewiesen.

5.1 Physikalische Kontrollen

Es müssen Maßnahmen beschrieben werden, die den Schutz der Infrastruktur erhöhen.

Die im Folgenden genannten Maßnahmen und Aufgaben unter 5.1 werden vom technischen Dienstleister erfüllt.

5.1.1. Standort und bauliche Maßnahmen (Dienstleister)

Die Zertifizierung beim technischen Dienstleister-wird innerhalb eines zugangsgesicherten Bereichs in einem weiteren Sicherheitsbereich betrieben. Der Sicherheitsbereich ist an ein Alarmsystem mit externem Alarm angeschlossen. Standorte und die technischen und baulichen Maßnahmen zum Schutz der CA sind detailliert in den nicht zur Veröffentlichung vorgesehenen Standortkonzepten beschrieben. Die Serverinfrastruktur befindet sich in zwei Rechenzentren. Die Offline CA – Umgebung befindet sich in einem gesondert gesicherten Bereich.

5.1.2 Physikalischer Zutritt

Zutritt erfolgt über ein mehrstufiges Zugangssystem. Die Zutrittskontrollanlage ist zusätzlich zu der Kontrollanlage des Gebäudes installiert. Dabei werden folgende Anforderungen berücksichtigt:

- 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

5.1.3 Stromversorgung und Klimatisierung

Es sind Maßnahmen zur Stromversorgung und Klimatisierung umgesetzt, die Stromversorgung ist auf die geforderte Verfügbarkeit der Sub-CA und der Leistungserbringer -Verfahren LE und dem Arbeitgeber-Verfahren (AGV) für die Erstellung von Benutzerzertifikaten abgestimmt.

5.1.4 Wasserschäden

Die Niederlassung verfügt über einen angemessenen Schutz vor Wasserschäden. Es sind keine stehenden oder fließenden Gewässer in der Nähe.

5.1.5 Brandschutz

Die geltenden Brandschutzbestimmungen werden eingehalten. Das Gebäude besitzt mehrere Brandabschnitte. Die Räume sind mit Rauch- und Brandmeldern ausgerüstet werden.

5.1.6 Aufbewahrung von Datenträgern

Datenträger mit kritischen Betriebsdaten sind vor Umwelteinflüssen geschützt gelagert. Hierfür wird ein Sicherheitsbereich aus einem anderen Brandabschnitts genutzt, der eine entsprechende physische Zutrittskontrolle besitzt.

5.1.7 Entsorgung

Dokumente und Datenträger werden fachgerecht entsorgt. Die Entsorgung wird entsprechend protokolliert.

5.1.8 Externe Sicherung

Von kritischen Daten werden Sicherheitskopien erzeugt und an einem anderen Standort in einem zweiten Brandabschnitt gesichert (siehe 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 (R)
- Zertifizierer (Z)
- HSM-Administrator (HA)
- Key-Manager (KM)
- Systemoperator (SO)

Diese Rollen sind in einem Rollenkonzept des Dienstleisters beschrieben und in einem Rollenzuordnungs-Dokument Mitarbeitern zugewiesen. Die Rollen dürfen nur mit geeigneten und vertrauenswürdigen Personen besetzt werden. Das Rollenkonzept wird vom Dienstleister verwaltet und regemäßig überprüft.

5.2.2 Anzahl der für eine Aufgabe erforderlichen Personen

Kritische Aufgaben, insbesondere Arbeiten mit dem privaten Schlüssel der CA, müssen im Vier-Augen-Prinzip durch Personen in der vertrauenswürdigen Rolle des Key-Managers des Dienstleisters durchgeführt werden. Dies gilt auch für Arbeiten an Komponenten wie HSM auf denen Schlüssel

erstellt oder verwaltet werden. Arbeiten an diesen Komponenten werden von mindestens zwei Mitarbeitern im Vier-Augen-Prinzip durchgeführt. Hierbei unterscheidet man ein technisch erzwungenes Vier-Augen-Prinzip wie bei einer gleichzeitigen Anmeldung von zwei Key-Managern an den HSMs und ein organisatorisches-technisches Vieraugen-Prinzip.

5.2.3 Identifizierung von Mitarbeitern für die Ausübung von Rollen

Mitarbeiter, die vertrauenswürdige Rollen übernehmen, müssen identifiziert werden und entsprechend 5.3.2 überprüft werden. Es muss sichergestellt sein, dass die Mitarbeiter identifiziert, werden, bevor sie:

- die Rolle nach 5.2.1 übernehmen und
- Zugang und
- Zugriff auf kritische Systeme und Einrichtungen erhalten.

5.2.4 Aufgabentrennung und Rollen

Auf eine Aufgabentrennung nach dem Rollenkonzept wird geachtet. Ein Mitarbeiter darf nur innerhalb einer dieser Bereiche eine Rolle übernehmen.

5.3 Personal

Die unter 5.3 aufgeführten Anforderungen werden vom technischen Dienstleister übernommen und erfüllt.

5.3.1 Anforderungen an Qualifikation, Erfahrung und Sicherheitsüberprüfung

Das TrustCenter setzt im Betrieb durch den technischen Dienstleister erfahrene Mitarbeiter in der PKI ein, die über die erforderlichen IT-Kenntnisse und insbesondere im CA–Betrieb verfügen. 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) sollte alle drei Jahre erneuert werden.

5.3.3 Schulung und Fortbildung

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

Abhängig vom Tätigkeitsbereich muss Basiswissen zu

- Public Key Infrastrukturen und Anforderungen an PKIs inklusive Key-Management

- Manipulationsmöglichkeiten von Dokumenten, Verifikationsprozesses und Bedrohungen durch Phishing und Social Engineering
- zum Datenschutz
- zur Meldung und zum Umgang mit Störungen vermitteln werden.

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 sein, dass durch einen Wechsel eines Arbeitsplatzes in unterschiedlichen Bereichen kein Rollenausschluss umgangen werden kann. Diese Anforderung wird über die Sicherheitskonzepte und insbesondere die Rollenkonzepten beachtet.

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 und zu disziplinarischen Folgen führen.

5.3.7 Anforderungen an unabhängige Auftragnehmer

Für externes Personal gelten die gleichen Sicherheitsanforderungen wie für die bereits für Mitarbeiter beschriebenen Anforderungen. Es muss ebenfalls ein polizeiliches Führungszeugnis (siehe Abschnitt 5.3.2) vorgelegt werden. Sie erhalten vor Beginn die gleichen Belehrungen und Unterweisungen wie Mitarbeiter.

5.3.8 Dokumentation, Schulungsunterlagen und Verfahrensanweisungen

Den Rolleninhabern stehen ausreichende Dokumentationen zur Erledigung ihrer Tätigkeiten zur Verfügung:

- Verfahrensbeschreibung
- Interne und externe Vereinbarungen
- Programmhandbücher
- Checklisten und Anleitungen
- Unterweisung durch langjährige Mitarbeiter

5.4 Protokollierung und Aufzeichnung von Ereignissen

Die unter 5.4 genannten Aufgaben wurden übertragen und werden vom technischen Dienstleister erfüllt.

5.4.1 Auszeichnung von Ereignissen

- Zertifizierungsanträge
- Registrierung von Benutzern
- Schlüsselerzeugungen für CA, PCA
- Zertifikatserzeugung für Sub-CA, PCA und Benutzer
- Datensicherung
- Zertifikatsveröffentlichung
- Erzeugung von Gesamtlisten
- Erzeugung von LDIF–Dateien
- Sperranträge
- Erstellung von Sperrlisten
- Veröffentlichung von Sperrlisten

Die Erfassung der Ereignisse erfolgt in der Regel durch manuell erstellte Protokolle, Datenbankeinträge und Systemlogs.

5.4.1.1 Lebenszyklus von Schlüsselpaaren

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

- Erstauftrag 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 alle 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 an Sicherheitsprofil
- Systemabstürze, Hardware-Ausfälle und andere Anomalien
- Firewall- und Router-Aktivitäten hinsichtlich Internetserver durch die Sicherheitsinfrastruktur
- Zutritt und Verlassen der gesicherten Umgebung (Protokollbuch)
- Direktes Monitoring der Server

5.4.2 Untersuchung von Protokollen

Protokolle und Datenbankeinträge werden auf sicherheits- und betriebsrelevante Ereignisse untersucht.

5.4.3 Aufbewahrungszeitraum für Audit-Protokolle

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

5.4.4 Schutz der Audit-Protokolle

Die Protokolldaten werden zusammen mit der Datenbank gesichert. Nachträgliche Änderungen sind nicht möglich.

5.4.5 Sicherungsverfahren für Audit-Protokolle

Auditprotokolle werden bedarfsweise gesichert.

5.4.6 Audit-Protokolle-Erfassungssystem

Protokoll-Datensätze werden direkt in der Datenbank erzeugt und abgelegt. Manuelle Dokumentationen von Prozessen und Ereignissen werden von den Mitarbeitern mittels Protokolle dokumentiert.

5.4.7 Benachrichtigung des ereignisauslösenden Subjekts

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

5.4.8 Schwachstellenprüfung

Die CA MUSS ihre Systeme regelmäßig mindestens quartalsmäßig auf Schwachstellen untersuchen. Die OFF- und Online System des Trustcenter stehen in abgesicherten Bereichen des technischen Dienstleisters werden auf quartalsmäßig auf Schwachstellen untersucht.

Das Sicherheitskonzept, die Anlagen und die Risikoanalysen für das Trustcenter werden regelmäßig durch den technischen Dienstleiter aktualisiert. Die internen und externen Bedrohungen, die zu unautorisierten Zugriffen, Veröffentlichung, Missbrauch, Austausch oder Zerstörung von Daten führen können werden identifiziert und die entstehenden Risiken bewertet und Maßnahmen geprüft.

Im Rahmen der Risikoanalyse muss ebenfalls überprüft werden, ob Vorgaben, Verfahren, Informationsverarbeitende Systeme und Technik, 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 in der Datenbank und vom CA-Server werden automatisch gesichert. Unterlagen werden manuell gesichert. Daneben wird das Auftauchen von verschiedenen Sicherheits-Events über das Monitoring gesichert und aktiv überwacht.

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Die vorgenannten Aufzeichnungen (Arten der archivierten Datensätze) müssen sechs Jahre aufbewahrt werden. Andere weitergehende gesetzliche Anforderungen müssen eingehalten werden.

5.5.3 Schutz von Archiven

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

5.5.4 Sicherungsverfahren

Archivdaten werden gegen unbefugte Lesezugriffe, Änderungen, Löschungen oder andere Manipulationen geschützt werden. 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 (siehe Abschnitt 5.5.1) dokumentiert werden, enthalten Informationen zu Datum und die 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

Für die Erstellung der End-Entity Zertifikate für die Benutzer sind die Sub-CA Zertifikate für die Verfahren LE und AGV bei der ITSG und LE der DKTIG maßgelblich.

Auf Grund der eingeschränkten Gültigkeit der CA-Zertifikate von 5 Jahren und der PCA-Zertifikate (Root-CA–Zertifikat) von 7 Jahren, ist regelmäßig (fast jährlich gegen Ende des Jahres) ein s.g. *Schlüsselwechsel* durchzuführen.

- *PCA CA Zertifikat* *7 Jahre*
- *CA–Zertifikat* *5 Jahre*
    - *Verfahren LE (ITSG)* *3 Jahre*
    - *Verfahren AGV* *3 Jahre*
    - *Verfahren LE (DKTIG)* *2 Jahre*

- *Benutzerzertifikate (LE und AGV)* *3 Jahre*
- *Benutzerzertifikate (DKTIG)* *2 Jahre*

Dabei werden für die betroffenen, auslaufenden CA-Zertifikate zunächst neue Schlüssel generiert und anschließend neue Zertifikate ausgestellt.

Die Zertifikate werden daraufhin den Verfahrensteilnehmern zur Verfügung gestellt und in den Gesamt- und Sammellisten veröffentlicht. Der Termin und das genaue Vorgehen eines jeden Schlüsselwechsels ist mit der ITSG und der DKTIG für einzelnen Verfahren entsprechend abzustimmen und mit ausreichend Vorlaufzeit bekanntzugeben und vorzubereiten.

Das allgemeine Vorgehen sowie die konkreten einzelnen, durchzuführenden Schritte sind im Betriebskonzept des CA-System sowie in der Schüsselzeremonie und den weiteren (von dieser referenzierten) Dokumenten zum Schlüsselwechsel beschrieben.

Beim Schlüsselwechsel von PCA und Sub-CA wird die Erzeugung der neuen Schlüssel und die Erstellung der neuen Zertifikate dokumentiert. So wird die Erstellung und Löschen von Schlüssel wird im Rahmen der Schlüsselzeremonie von den Key-Managern dokumentiert.

An dem Schlüsselwechsel nehmen nur authentifizierte Mitarbeiter entsprechend ihren Rollen aus dem Rollenkonzept teil. Die Rollen werden transparent gemäß Rollenkonzepten und Rollenzuordnungen dokumentiert.

Das allgemeine Vorgehen sowie die konkreten einzelnen, durchzuführenden Schritte sind in der Dokumentation der Schüsselzeremonie und den weiteren (von dieser referenzierten) Dokumenten zum Schlüsselwechsel und den Dokumentationen für die Erzeugung neuer Schlüssel auf HSMs beschrieben.

Zertifikatsprüfung, Freigabe und Konfiguration der neuen Schlüssel

Die neuen Zertifikate und Fingerprints werden zusammen mit den Auftraggebern inhaltlich geprüft und nach Freigabe in der produktiven Umgebung installiert und auf den Webseiten veröffentlicht (Siehe auch Abschnitt 2 zu dem Thema „Verzeichnis und Veröffentlichung“).

Vor der Freigabe der gesamten Produktionsumgebung werden entsprechend Tests durchgeführt und die Schlüssel geprüft.

5.7 Kompromittierung und Wiederherstellung des Betriebes

Die Certificate Authorities müssen über eine Geschäftsfortführungsplanung (business continuing plan) verfügen, um den Geschäftsbetrieb bei Ausfällen oder Krisensituationen zu gewährleisten.

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

Die Systeme werden über Datensicherungen neu aufgesetzt und in Betrieb genommen.

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. Dies gilt auch für die durch die Zertifizierungsstellen erstellten Endnutzer-Zertifikate.

Die PKI nutzt das **Whitelist**-Verfahren. Täglich 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. Daneben werden auch Sperrlisten erstellt und veröffentlicht. Die Endnutzer müssen hierfür über die Webseiten oder direkt per Mail informiert werden. Sie werden u.a. dazu aufgefordert neue Zertifikatsanträge zu stellen.

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 für die Business Continuity (Voraussetzung und Prüfung des Eintritts des Notfall-Szenario)
- die Notfallprozesse (Fallback)
- Wiederaufnahmepläne
- Sensibilisierung und Wissensanforderungen bei Mitarbeitern
- Vorgaben für die Wiederherstellungszeiten
- Einen Zeitplan zur Wiederherstellung bzw. Wiederaufnahme des Geschäftsbetriebes nach einem Fehler oder Ausfall.
- Eine Anforderung kritisches kryptografisches Material (e.g. HSM) an einem alternativen Ort zu lagern.
- 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

Die CA und insbesondere der technische Dienstleister muss einen Notfallplan für die Fortführung des Betriebs 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 CA ab.

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

Bei einer Kompromittierung des privaten Schlüssels des Teilnehmers muss die PKI die notwenigen Schritte für die Sperrung des Endnutzerzertifikat eingeleitet werden. Der Antragsteller muss nach der Sperrung einen neuen Antrag an die PKI stellen.

5.7.4 Geschäftskontinuität nach einem Notfall

Die CA 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 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 CA oder RA-Betriebes

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

- Dies umfasst insbesondere die Mitteilung der Betriebseinstellung.
- Es muss Erklärung für die Übernahme oder Bereitstellung von Geldmitteln für die Kosten der Einstellung, Abwicklung oder Übertragung der gültigen Zertifikate auf eine andere CA 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 Endnutzerzertifikate

Für die Endnutzerzertifikate gilt, dass der Antragsteller den öffentlichen und den privaten Schlüssel erstellt. Der Antragsteller bzw. Ansprechpartner ist dafür verantwortlich, dass der private Schlüssel gesichert vor Zugriffen Dritter aufbewahrt wird.

6.1.1.2 Generierung von RA- Schlüsselpaaren

(Nichtzutreffend)

6.1.1.3 Generierung von Subscriber-Schlüsselpaaren (EE-Zertifikate) für Endnutzer der Verfahren LE und AGV der ITSG und DKTIG

Der Zertifikatnehmer ist verantwortlich die eigenen Schlüssel entsprechend den Vorgaben sicher zu erzeugen und insbesondere den privaten Schlüssel sicher zu verwahren. Private Schlüssel werden vom TrustCenter weder für Zertifikatsnehmer erstellt, verwahrt noch ausgeliefert.

6.1.2 Bereitstellung des privaten Schlüssels an Zertifikatsnehmer

(Nichtzutreffend) Der Antragsteller erstellt die Schlüssel für das Endnutzerzertifikat.

6.1.3 Bereitstellung des öffentlichen Schlüssels an die Zertifizierungsstelle

Für den Zertifikatsantrag wird der öffentliche Schlüssel an die Zertifikatsstelle als Teil des Requests auf einem sicheren Weg übermittelt.

6.1.4 Bereitstellung der öffentlichen PCA, CA und der Schlüssel des Endnutzers

Eine Bereitstellung erfolgt:

- durch eine Veröffentlichung auf den Webseiten der nachgeordneten Certificate Authorities
- direkt über den Download der PCA und CA-Zertifikate
- über den Abruf der Gesamtlisten
- sowie dem Laden von LDIF-Datei.

6.1.5 Algorithmen und Schlüssellängen

Für vollständige Darstellung wird auf die technischen Vorgaben für die PCA und die nachgeordneten „Certificate Authorities“ auf die „Anlage 16“ der „Gemeinsame Grundsätze Technik“ des GKV verwiesen.

Es werden folgende Verschlüsselungsalgorithmus verwendet.

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)

Hashalgorithmus (SHA)	Message Digest“	SHA-256	[OID 2.16.840.1.101.3.4.2.1]	RFC8017	Anlage 16-2.1.1.
Signaturalgorithmus	Signatur Algorithms	id-RSASSA-PSS	[OID 1.2.840.113549.1.1.10]	RFC8017	Anlage 16-2.1.2
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 16-2.1.3

6.1.6 Generierung öffentlicher Schlüsselparameter und Qualitätskontrolle

Es werden die Schlüsselalgorithmen aus der Tabelle zu 6.1.5 erwartet.

6.1.7 Bestimmung der Schlüsselverwendung

Private CA-Schlüssel des Antragstellers werden ausschließlich zum Signieren der Zertifikats-Request verwendet.

6.2 Schutz privater Schlüssel und technische Kontrollen kryptografischer Module

6.2.1 Standards und Kontrollen für kryptografische Module

Die privaten Schlüssel der Root-CA und der Sub-CA werden verschlüsselt in kryptographischen Modulen für die Zertifizierung hinterlegt. Das CA-System wird ohne Netzanschluss nach Außen offline in einem Sicherheitsbereich betrieben.

6.2.2 Vier-Augen-Prinzip bei privaten Schlüsseln

Die Kontrolle der Nutzung von privaten Schlüsseln ist durch das Vier-Augen-Prinzip geschützt. Die Ausführung von Aktionen und der Zugriff wird technisch oder organisatorisch so beschränkt, dass beim technischen Dienstleiter mindestens 2 Mitarbeiter für den direkten Zugriff notwendig sind. Zugriff und die Rollen für das Erstellen von Schlüsseln haben nur langjährige Mitarbeiter, die die Rolle, Schulung und Erfahrung als Key-Managers haben.

6.2.3 Hinterlegung von privaten Schlüsseln

(Nichtzutreffend). Eine Hinterlegung von privatem Schlüssel für Antragsteller wird nicht durchgeführt.

6.2.4 Sicherung (Key-Backup) von privaten Schlüsseln

(Nichtzutreffend). Es werden keine privaten Schlüssel der Antragsteller gesichert.

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 Sperrung noch 10 Jahre aufbewahrt. Details regelt das Löschkonzept.

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 Master-Backup-Key wird im Rahmen einer Schlüsselzeremonie im Vier-Augenprinzip (siehe Abschnitt 6.2.4) durchgeführt. Die Übertragung von privaten Schlüsseln erfolgt nur verschlüsselt mit dem MBK. Übertragungen erfolgen nur zu Backup- oder Wiederherstellungszwecken. Von Antragstellern erhält das Trustcenter nur die Requests zu Erstellung der Zertifikate. Der private Schlüssel muss von dem Antragsteller gesichert aufbewahrt werden.

6.2.7 Speicherung privater Schlüssel auf kryptografischen Modulen

Das Schlüsselpaar wird in einem kryptografischen gesicherten Modul gespeichert.

6.2.8 Aktivierung privater PCA-Schlüssel auf kryptografischen Modulen

Die Erstellung und Aktivierung der Root-CA-Schlüssel müssen durch mehrere Personen (2 Key-Manager) durchgeführt werden. Mit der Erstellung im kryptographischen Modul wird der Schlüssel aktiviert.

6.2.9 Deaktivierung privater Sub-CA-Schlüssel auf kryptografischen Modulen

Die Deaktivierung eines Schlüssels erfolgt ebenfalls im kryptographischen Modul im Rahmen einer „Key Ceremony“.

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.

6.3 Aspekte zur Verwaltung von Schlüsselpaaren

6.3.1 Archivierung von öffentlichen Schlüsseln

Die Archivierung von PCA und CA-Schlüsseln wird durch mehrere Personen im Vier-Augen-Prinzip durchzuführen und dokumentiert.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

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

7 Profile von Zertifikaten und Sperrlisten

7.1 Versionsnummer

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

7.2 X.509 Zertifikate und Erweiterungen

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 enthalten folgen Erweiterungen

Key Usage

- Extend Key Usage
- Basic Constraints CA=false, keine Pfadlängenbeschränkung

Authority Key Identifier

- Identifizierung von Zertifizierungsstellenzertifikate bzw. Ausstellerzertifikaten
- Der AuthorityKeyIdentifier (AKI) dient der Sicherstellung des Aufbaus eines Zertifizierungspfades bei der Zertifikatsvalidierung und ermöglicht eine Referenz auf das Ausstellerzertifikat.
  Der in der ***AKI-Erweiterung*** angegebene Wert im Feld *keyIdentifier* muss identisch sein mit dem Wert *keyIdentifie*r der ***SKI-Erweiterung*** des Ausstellerzertifikat.
- Die Erweiterung ist in allen CA-Zertifikaten enthalten.
- Alle neuen Teilnehmer-Zertifikate, die von einer CA ab dem vierten Quartal 2021 zertifiziert werden, müssen diese Erweiterung enthalten.
- Seriennummern werden nicht zweimal vergeben und sind damit eindeutig.

7.3. Sperrlistenprofil

7.3.1 Bereitstellung

Die Definition der Profile für Zertifikate und Sperrlisten entspricht den MTTv2-Spezifikationen.

Die Sperrlisten werden in regelmäßigen Abständen (bei jeder Änderung) innerhalb des Verzeichnisdienstes veröffentlicht. Die Teilnehmer der PKI erhalten die Sperrlisten täglich mit den aktuellen Gesamtlisten, die alle gültigen Zertifikate enthalten.

7.3.2 Verarbeitung von Sperrlisten

Jeder Teilnehmer muss die Verarbeitung von Sperrlisten (Certificate Revocation List, CRL) unterstützen. Dazu sind die folgenden Funktionalitäten bereitzustellen:

- Anforderung zur Sperrung eines Zertifikats
- Anforderung von Sperrlisten von einer CA
- Verifizierung von Sperrlisten, um deren Echtheit zu gewährleisten (Sperrlisten sind von der jeweiligen CA signiert)
- Periodisches Überprüfen des Gültigkeitszeitraums einer Sperrliste und Anfordern einer neuen Sperrliste
- Echtheits-Verifizierung von Sperrlisten (Sperrlisten sind von der CA signiert), periodisches
- Überprüfen des Gültigkeitszeitraums einer Sperrliste (dadurch kann das Anfordern einer neuen Sperrliste ausgelöst werden).

7.4 OCSP-Profil

(Nichtzutreffend). OCSP wird nicht unterstützt.

8 Konformitätsprüfung

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

Die Einhaltung, Dokumentation und Aktualität der Maßnahmen des Sicherheitskonzeptes werden beim Dienstleister jährlich im Rahmen einer dedizierten Auditierung des Trustcenter nach ISO 27001 von einer externen, akkreditierten Stelle überprüft und in einer entsprechenden Urkunde bestätigt.

8.1 Frequenz und Umstände der Überprüfung

Interne und externe Audits beim Dienstleister werden in regelmäßigen Abständen durchgeführt.

8.2 Identität und Qualifikation des Prüfers

Die Prüfer verfügen 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

Festgestellte Mängel müssen in Abstimmung zwischen Zertifizierungsstelle und Prüfer zeitnah beseitigt werden. Die Prüfer werden über die Beseitigung der Mängel informiert.

8.6 Veröffentlichung der Ergebnisse

Eine Veröffentlichung der Prüfungsergebnisse ist nicht vorgesehen.

9 Weitere geschäftliche und rechtliche Regelungen

9.1 Gebühren

Detaillierte Informationen befinden sich in den Verträgen zwischen der Zertifizierungsstelle und dem Antragsteller sowie in den bestehenden Verträgen zwischen CA und Dienstleister.

9.2 Finanzielle Verantwortung

Risiken, die aus der Haftung für eine CA entstehen können, müssen abgedeckt werden. Diese Absicherung kann auch mittels Haftpflichtversicherung geschehen.

9.3 Vertraulichkeit von Geschäftsinformationen

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

Dieses gilt nicht so weit die Daten direkt den Inhalt des Zertifikats betreffen oder aus den Zertifikaten abgeleitet werden können. Einschränkung der Vertraulichkeit und des Datenschutz nach 9.3.2.

9.3.2 Daten und Informationen, die in den herausgegebenen Zertifikaten

Informationen, die in Sperrlisten und Zertifikaten enthalten sind oder davon abgeleitet werden können, werden ebenfalls nicht als 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 stimmt der Nutzung von personenbezogenen Daten durch die PKI zu, sowie dies zur Leistungserbringung erforderlich ist. Als nicht vertraulichen Informationen werden alle Informationen eingestuft, die in den zu veröffentlichenden Zertifikaten, Sperrlisten und Statusinformationen enthalten sind oder davon abgeleitet werden können.

9.5 Urheberrechte

(Nichtzutreffend)

9.6 Verpflichtungen

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

Die Verpflichtung des Zertifikatsnehmers für ausschließlich eigene Nutzung des privaten Schlüssels ist in Ziffer 4.5.1 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.

9.9 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 CPS tritt an dem Tag in Kraft, an dem es veröffentlicht wird (s. Abschnitt 2.3).
Dieses Dokument ist gültig, bis es durch eine neue veröffentlichte Version ersetzt wird oder Betrieb der PKI eingestellt wird.

Die Verantwortung für den Schutz vertraulicher Informationen und personenbezogener Daten bleibt unberührt. Es gelten die Beschränkungen aus Abschnitt 9.3.2...

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

In dieser Zertifizierungsrichtlinie werden keine entsprechenden Regelungen getroffen.

9.12 Änderungen der Richtlinie

Änderungen der CPS werden rechtzeitig vor ihrem Inkrafttreten veröffentlicht (s. Abschnitt 2.3).

9.13 Schiedsverfahren

(Nichtzutreffend)

9.14 Gerichtsstand

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

9.15 Konformität mit geltendem Recht

Es gilt deutsches Recht.

9.16 Weitere Regelungen

Die Regelungen der CPS gelten zwischen der PKI und den Zertifikatsnehmern. Zertifikatsnehmer sind die Antragsteller.

[Salvatorische Klausel]
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 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)
- TR 3107-1 Elektronische Identitäten und Vertrauensdienste im E-Government

10 Abkürzungen

Abkürzung	Definition – Beschreibung
ITSG	Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH
DKTIG	Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH
DKG	Deutsche Krankenhausgesellschaft e.V.
GKV	Gesetzliche Krankenversicherung
GKV-SV	GKV-Spitzenverband – Spitzenverband Bund der Krankenkassen (gemäß §217a SGB V)
RA	Registration Authority – Registrierungsinstanz zur Legitimation von Teilnehmern und Anträgen
CA	Certification Authority – Zertifizierungsinstanz zur Ausstellung von Zertifikaten
PCA	Policy CA / Root-CA – Der Vertrauensanker des Sicherheitsverfahrens

Abkürzung	Definition – Beschreibung
TC	Trust Center – Vertrauensstelle, Betreiber einer RA und CA bzw. PCA
DALE, LE	Datenaustausch im Leistungserbringerverfahren
AGV	Arbeitgeber-Verfahren
DB	Database / Datenbank
OID	Object Identifier – Bezeichner für Informationsobjekte (nach ISO/IEC 9834)
ASN.1	Abstract Syntax Notation One – Beschreibungssprache zur Definition von Datenstrukturen
BER / CER / DER	Basic / Canonical / Distinguished Encoding Rules – Verschiedene Kodierungsvorschriften für Daten im ASN.1-Format (nach X.690)
CMS	Cryptographic Message Syntax – Nachrichtenformat zum Austausch signierter oder verschlüsselter Inhalte
CRQ	Certification Request – Elektronische Zertifizierungsanfrage
CRP	Certification Response – Elektronische Zertifizierungsantwort
CRL	Certificate Revokation List – Eine Liste gesperrter Zertifikate
FTP	File Transfer Protocol – Ein Kommunikationsprotokoll zur Übertragung von Daten