Historie

Version	Stand	Bearbeiter	Änderung / Kommentar
1.00	23.12.2023	Christoph Luxem	Initiale Version

Inhaltsverzeichnis

1 Einleitung

1.1 Überblick

Dieses Dokument fasst die verbindlichen Zertifizierungsrichtlinien der Public Key Infrastructure (im folgenden PKI) für die Ausstellung von Zertifikaten zur Verschlüsselung und Authentisierung in Form einer Certificate Policy (CP) zusammen.

Die oberste Zertifizierungsstelle wird als PCA (Policy Certification Authority) bezeichnet. Im folgenden Dokument wird Policy Certification Authority mit PCA abgekürzt.

Die von den Spitzenverbänden der gesetzlichen Krankenkassen eingerichtete

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

haben sich auf eine gemeinsame Gestaltung der 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 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 (DALE)
- CA: DKTIG TrustCenter für Krankenhäuser und Leistungserbringer PKC (DKTIG).

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“.

Änderungen der inhaltlichen und fachlichen Anforderungen werden von den beteiligten Parteien und dem Spitzenverband (GKV) abgestimmt.

1.1.1 ITSG GmbH

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

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

1.1.2 DKTIG GmbH

Die Schlüsselverzeichnisse der Annahmestellen (§ 301 SGB V Datenübermittlung) der GKV und der PKV können auf der Homepage des TrustCenter der DKTIG *(Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH)* runtergeladen werden:

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

1.2 Die Gliederung des Dokumentes erfolgt nach dem Standard des RFC 3647

Name:	Certificate Policy (CP) für das Leistungserbringer (DALE), Arbeitgeberverfahren (AGV) für das Datenübertragungsverfahren nach § 301 SGB V für den Zugang der Krankenhäuser sowie Vorsorge- und Rehabilitationseinrichtungen.
Version:	1.00
Datum:	23.12.2023
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 als Zertifizierungszertifikate in Zertifizierungsstellen.

Die fachlichen Zertifizierungsstellen für

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

werden von der „*ITSG Informationstechnische Servicestelle der gesetzlichen Krankenversicherung GmbH*“ betrieben.

Die fachliche Zertifizierungsstelle für

- das Verfahren der Datenübertragung gem. § 301 SGB V für den Zugang der Krankenhäuser sowie Vorsorge- und Rehabilitationseinrichtungen

wird von der „*DKTIG Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH*“

betrieben.

Die genannten Zertifizierungsstellen erstellen die Endnutzerzertifikate für die sichere Kommunikation im Gesundheits- und Sozialwesen.

Kontaktadressen:

Kontaktdaten: DKTIG

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

Homepage: www.dktig.de

- Service portal: www.dktig-serviceportal.de
    - Anmeldung zur Online-Status-Zertifizierung https://www.dktig-trust.de/dktig/osa.php
    - 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 CP-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 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“ eine Tochter der „Atos Information Technology GmbH“ betraut.

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 öffentlichen Schlüsselverzeichnisse, 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 CP-Dokument

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

1.5.2 Ansprechpartner und Kontakte

Kontaktinformationen ITSG

- Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH (ITSG)
- Die kostenlose 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/

Kontaktinformationen DKTIG:

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

1.5.3 Prüfung der Zertifizierungsrichtlinie

Diese Certificate Policy (CP) wird einem jährlichen Review unterzogen. Daneben erfolgt eine Überprüfung bei besonderen Anlässen. Änderungen und Review werden in der Änderungshistorie vermerkt, auch wenn keine inhaltlichen Änderungen vorgenommen werden.

1.5.4 Veröffentlichung der Zertifikatsrichtlinien

Die CP 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 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 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 verschiedenen Verfahren DALE, AGV 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 hierarchisch unter den Sub-CA-Zertifikaten zu finden, 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/

- Teilnehmer-Zertifikate für
    - Arbeitgeberverfahren mit Fingerprint
    - Leistungserbringerverfahren mit Fingerprint
    - 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/

- Teilnehmer-Zertifikate für Leistungserbringerverfahren mit Fingerprint
- 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-Directorys 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:

PCA der Trust Center

PCA für das Arbeitgeber- und Leistungserbringerverfahren	Tag des Schlüsselwechsels

ITSG

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

DKTIG CA (mit Fingerprint)	Tag des Schlüsselwechsels
Certificate Policies	Nach Erstellung bzw. Aktualisierung und Freigabe
Certification Practice Statement	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 öffentlichen Schlüsselverzeichnisse 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

Zertifizierungsstellen und nachgeordnete CA:

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

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

- Seriennummer (dc): 80/(hex): 50
- Gültigkeitszeitraum: 30.11.2021 bis 30.01.2029
- Signaturhashalgorithmus: SHA256
- Signaturalgorithmus: RSASSA-PSS
- Schlüssellänge: RSA 4096 Bits
- SHA1-Fingerprint: 6476a953c92e279776875cf1b52b3a7bdfb1d874

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

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

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

(1) ZERTIFIKATE MIT RSASSA-PSS-SIGNATURALGORITHMUS

- Seriennummer (dc): 52/ (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):55 / (hex): 55
- Gültigkeitszeitraum: 28.11.2023 bis 07.01.2029
- Signaturhashalgorithmus: SHA256
- Signaturalgorithmus: RSASSA-PSS
- Schlüssellänge: RSA 4096 Bits
- SHA1-Fingerprint: 1298f7e78a42133c52b6b4c01d0ee1703f75d6cb

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

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

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

(1) ZERTIFIKATE MIT RSASSA-PSS-SIGNATURALGORITHMUS

- Seriennummer (dc):51 / (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

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

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

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

(1)

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

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

(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/

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).

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 Krankenhäuser und Leistungserbringer (PKC)“
3	Organization-UnitName (verpflichtend)	OU	Name der Institution (Firmenname des Leistungserbringes 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 Felds „subject“ ist gewährleistet, um eine Feststellung des Zertifikatsinhabers ohne Verwechslungsgefahr zu ermöglichen. Der Namen 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 Betriebsnummer - oder ein Institutionskennzeichen haben, erfolgt eine Feststellung der Organisation durch die „*ARGE IK*“ oder die „*Bundesagentur für Arbeit*“ im Rahmen der Vergabe der -Nummer.

3.2.3 Authentifizierung natürlicher Personen

Für die Authentifizierung natürliche 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 DALE und AGV)
- Postident-Verfahren und zweiter Faktor (DKTIG)

3.2.4 Nicht überprüfte Zertifikatsnehmer Informationen

Es werden alle Angaben zur Authentifikation und Identifikation von Zertifikatsnehmers durch das Trustcenter überprüft. Betriebsnummern und Institutionskennzeichen werden anhand von Firmendaten der ARGE IK und „Bundesagentur für Arbeit „überprüft“. Andere oder zusätzliche Informationen des Zertifikatsnehmers 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.

Die Autorisierung einer natürlichen Person als Handlungsberechtigter im Namen einer Organisation erfolgt organisationsintern nach einem dafür geeigneten und vorgesehen 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 „Bundesagentur 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 Bundesagentur 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 bei einer Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung und Folgezertifikat

3.3.1.1 Zertifikatserneuerung

Die Zertifikatsnehmer werden vor Ablauf der Gültigkeit des Zertifikats zur Zertifikatserneuerung aufgefordert. Die Identifizierung und Authentifizierung erfolgt entsprechend zum initialen Antragsprozess.

3.3.1.2 Zertifikatserneuerung durch Folgezertifikat (nur ITSG)

Der Antragssteller kann mit einem gültigen Zertifikat ein Folgezertifikat beantragen. Ein Folgeantrag ist ein Antrag, der auf Grundlage einer bereits abgeschlossenen Identifizierung eines anderen Antrags gestellt wird. Bei einem Folgeantrag können die bei einem Erstantrag angefallenen Daten wieder

verwendet werden. Auf neue Identifizierung und Authentifizierung kann nur verzichtet werden, wenn sich neben den Antragsdaten insbesondere 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 ist 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.).

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

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 Zertifikate können von den Zertifikatsnutzern nach Abschnitt 1.3.3 gestellt werden.

Der Zertifikatsantragsprozess 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 Registrierungsprozess. Folgende Prüfungen werden durchgeführt, ob alle erforderlichen Antragskomponenten übermittelt, wurden:

- Prüfung der Berechtigung des Antragstellers
- Vollständigkeit und Korrektheit des Antrags
- Eindeutigkeit des DN
- Übereinstimmung der Antragsdaten und der Daten im PKCS#10-Request
- Technische Prüfung des PKCS#10-Request inkl. Hashwert / Fingerprint

- Prüfung der Authentizität

4.1.3 Zertifikatsantrag

Der Zertifikatsantrag für Endnutzerzertifikate in den Verfahren Dale, AGV und dem DKTIG-Verfahren nach §301 SGB V besteht ausfolgenden Daten:

Verfahren DALE und AGV der ITSG

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

Ablauf des Zertifikatsantragsverfahren DALE und AGV:

- allgemeine Informationen: https://www.itsg.de/produkte/trust-center/zertifikat-beantragen/
- Zertifizierungsablauf: https://www.itsg.de/produkte/trust-center/unterlagen-download/
- Registrierungsportal der ITSG (https://registrierungsportal.itsg.de/regportal/client/de/login)
- sowie dem vom Antragsteller genutzten elektronischen Programm für die Antragsstellung.

Verfahren der DKTIG nach §301 SGB V

- Name der Einrichtung
- Adresse
- Institutionskennzeichen
- Ansprechpartner (Schlüsselverantwortlicher)
- Benötigte Kontaktdaten des Ansprechpartners (Schlüsselverantwortlichen)
    - Telefon
    - E-Mail
    - Abteilung
- Datenschutzeinwilligung

Ablauf des Zertifikatsantragsverfahren nach §301 SGB V:

- Ablauf der Beantragung der Zertifikat nach § 301 SGB V: Zertifikat beantragen - DKTIG
- Zertifizierungsablauf: https://dktig.de/zertifizierungsablauf/
    - Detaillierter Ablauf: Zertifizierungsablauf_2023.pdf
    - Antragsformular: Formular Zertifikatsanforderung.pdf

4.2 Bearbeitung von Zertifikatsanträgen

4.2.1 Durchführung der Identifikation und Authentifizierung

Der Antragsteller 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 Zertifikatsanträgen bis zur Veröffentlichung beträgt bis zu sieben Tage.

4.3 Ausstellung von Zertifikaten

4.3.1 Tätigkeiten während der Ausstellung von Zertifikaten

Nach der Bearbeitung der Zertifikatsanträge werden die neuen Zertifikate für die Antragsteller erstellt. Die Ausstellung von Endnutzerzertifikaten unterliegt festgelegten Prüfungen und wird dokumentiert und protokolliert.

Die Zertifikate werden nach der Erstellung nochmal mit dem Antrags- und den Authentifizierungsunterlagen verglichen.

4.3.2 Erstellung, Benachrichtigung, Bereitstellung und Veröffentlichung der Zertifikate

Die Antragsteller werden über die Erstellung und Bereitstellung des beantragten Zertifikates benachrichtigt. Die Bereitstellung des Zertifikates für den Antragsteller erfolgt entsprechend dem von ihm gewählten Antragsweg.

Die Zertifikate werden zusätzlich über die öffentlichen Schlüsselverzeichnisse für die Teilnehmer der PKI veröffentlicht.

Die Bereitstellung des Zertifikates für den Antragsteller erfolgt entsprechend dem von ihm gewählten Antragsweg.

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. Die Annahmebestätigung durch den Antragsteller sollte innerhalb einer bestimmten Frist erfolgen.

4.4.2 Veröffentlichung des Zertifikates durch die CA

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

4.4.3 Benachrichtigung weiter Instanzen durch die CA

(Nichtzutreffend)

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Nutzung des privaten Schlüssels

Die Nutzung des privaten Schlüssels darf ausschließlich durch den Antragsteller als Zertifikatsnehmer möglich sein. Der Zertifikatsnehmer kann einen Dienstleister zur Nutzung des privaten Schlüssels beauftragen. Für die Sicherheit der privaten Schlüssel hat der Zertifikatsnehmer 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 Zertifikatsauftraggeber

(Nichtzutreffend)

4.6.5 Annahme.

Es gelten die Regelungen gemäß Abschnitt 4.4 zur Zertifikatsakzeptanz.

4.6.6 Veröffentlichung

Es gelten die Regelungen zur Veröffentlichung gemäß Abschnitt (4.4.2).

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

(Nichtzutreffend)

4.7 Zertifikatserneuerung mit Schlüsselwechsel (Re-Keying)

Bei der Zertifikatserneuerung wird immer ein neues 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 wird in der Regel mit *Schlüsselwechsel* und einer *Zertifikatserneuerung* durchgeführt. Im Rahmen der Zertifikatserneuerung werden die Zertifikatsinhalte und die verwendeten technische 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 den Festlegungen zu der Laufzeit der PCA und den untergeordneten Zertifizierungsstellenzertifikaten sowie deren Nutzungs- und Gültigkeitsdauern aufgrund des verwendeten Schalenmodells.

Daneben kann eine außerplanmäßige Zertifikatserneuerung ebenfalls von den Zertifikatsnehmern 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. Der Zertifikatsnehmer wird über die Erstellung des Zertifikates informiert. Eingehalten werden müssen auch 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. Die Nutzung eines Zertifikats obliegt dem Zertifikatsnehmer.

4.8.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle

Die neuen Zertifikate werden den Gesamtlisten hinzugefügt und werktäglich veröffentlicht. Ungültige oder gesperrte Zertifikate werden aus den Gesamtlisten gelöscht und werktäglich 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.

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 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 die Sperrung seines eigenen Zertifikates beantragen.

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 Sperrlisten und die Gesamtlisten.

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 Zug 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 die werktägliche Erzeugung und Verteilung von Gesamtlisten sicher, dass die gültigen Zertifikate in Format der Gesamtlisten für die PKI nutzenden Beteiligten bereitstehen.

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

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Sperrlisten werden werktäglich neu erzeugt und veröffentlicht.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die Sperrlisten werden werktäglich zusammen mit den Gesamtlisten für die Teilnehmer der PKI öffentlich bereitgestellt.

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. 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 direkt die betroffenen Zertifikate unwiderruflich gesperrt und nicht suspendiert. Eine temporäre Sperrung wird nicht genutzt.

4.9.14 Beantragung einer Suspendierung
Keine Antragsmöglichkeit.

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 den PKI-Teilnehmern werktäglich 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

Hinsichtlich der nicht technischen Sicherheitsmaßnahmen wird auf das CPS verwiesen.

6.Technische Sicherheitsmaßnahmen

Hinsichtlich der technischen Sicherheitsmaßnahmen wird auf das CPS verwiesen.

7 Profile von Zertifikaten und Sperrlisten

Hinsichtlich der Profile von Zertifikaten und Sperrlisten wird auf das CPS verwiesen.

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.

8.1 Frequenz und Umstände der Überprüfung

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

8.2 Identität und Qualifikation des Prüfers

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

8.3 Verhältnis von Prüfer zu Überprüftem

Die Prüfer dürfen nicht in den Produktionsprozess eingebunden sein.

8.4 Überprüfte Bereiche

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

8.5 Mängelbeseitigung

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 Antragsunterlagen und öffentlichen Information der Zertifizierungsstellen.

9.2 Finanzielle Verantwortung

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

9.3 Vertraulichkeit von Geschäftsinformationen

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

Dieses gilt nicht so weit die Daten direkt den Inhalt des Zertifikats betreffen. 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 abgeleitete werden können, werden als nicht vertraulich eingestuft.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

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

9.4 Schutz personenbezogener Daten

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

Daten über Zertifikatsnehmer und Teilnehmer werden vertraulich behandelt.

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

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

9.5 Urheberrechte

(Nichtzutreffend)

9.6 Verpflichtungen

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

Die Verpflichtung des Zertifikatsnehmers 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.

Die vorstehende Haftungsbeschränkung gilt auch für die persönliche Haftung der Mitarbeiter, Vertreter und Organe des Anbieters.

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 eines Antragstellers ist die PKI von der Haftung freigestellt.

9.10 Inkrafttreten und Aufhebung

Diese CP tritt an dem Tag in Kraft, an dem es veröffentlicht wird (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 CP werden rechtzeitig vor ihrem Inkrafttreten veröffentlicht (s. Abschnitt 2.3).

9.13 Schiedsverfahren

(Nichtzutreffend)

9.14 Gerichtsstand

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

9.15 Konformität mit geltendem Recht

Es gilt deutsches Recht.

9.16 Weitere Regelungen

Die Regelungen der CP gelten zwischen der PKI und den Zertifikatsnehmern. Zertifikatsnehmer 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 CP, 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

C	Country (Bestandteil des Distinguished Name)
CA	Certification Authority, Zertifizierungsinstanz
CN	Common Name (Bestandteil des Distinguished Name)
CP	Certificate Policy; Zertifizierungsrichtlinie einer PKI
CPS	Certification Practice Statement, Regelungen für den Zertifizierungsbetrieb
CRL	Sperrliste
(CRL) CDP	Extension Sperrlistenverteilungspunkte
DN	Distinguished Name
E-Mail	E-Mail Address
HSM	Hardware Security Module (hier: Sicherung der Root CA und Sub CA Schlüssel)
http	Hypertext Transfer Protocol
https	Hypertext Transfer Protocol Secure
ISMS	Information Security Management Protokoll (Management System für Informationssicherheit

O	Organisation (Bestandteil des Distinguished Name)
OID	Object Identifier
OU	Organizational Unit (Bestandteil des Distinguished Name)
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PSE	Personal Security Environment
RA	Registration Authority, Registrierungsstelle
RFC	Request for Comment, Dokumente für weltweite Standardisierungen
Root-CA	Obererste Zertifizierungsinstanz einer PKI
S/MIME	Secure Multipurpose Internet Mail Extension