Zertifizierungsrichtlinie (Certificate Policy) Abrechnungszentrum Emmendingen

Version: 4.0

Stand: 28.12.2020

Status: Freigegeben

Verantwortlicher: Michael Künzler

Klassifizierung: C1 - Öffentlich

Inhaltsverzeichnis

Verzeichnis der Tabellen:

Dokumentenhistorie

Version	Datum	Autor(en)	Durchgeführte Änderungen
0.1	09.03.18	Michael Kromer	Erstellung erster Entwurf
0.2	27.04.18	Michael Kromer	Anpassungen
0.3	27.04.18	Reinhard Habichtsberg	Überarbeitung Kapiteleinteilung und Inhaltsverzeichnis
0.5	07.09.18	Michael Kromer	Anpassungen
0.6	25.10.18	Uwe Bührer	„aktive EZT“ entfernt und der „passive EZT“ in „EZT“ umbenannt. Geändert: Kap. 5.1.1, 5.2.2, 6.5, 8.1.1
0.7	02.11.18	Michael Künzler	Umstellung auf Formatvorlage für Sicherheitsrichtlinien (SharePoint)
1.0	07.11.18	Michael Künzler	Fertigstellung der ersten Hauptversion zu Freigabe durch die Geschäftsführung.
2.0	08.11.18	Michael Künzler	Verzeichnis der Tabellen hinzugefügt und Kapitel 5 und 6 überarbeitet.
3.0	10.01.19	Michael Künzler	Review durch Herrn Scharbach. (Kapitel 3.2.7 entfernt und Tabelle 11 in Kapitel 8.8.1. angepasst. Freigabe zur Veröffentlichung.
4.0	28.12.2020	Michael Künzler	Jährliches Review mit kleinen redaktionellen Änderungen. Freigabe zur Veröffentlichung.

1 Einleitung

Das Abrechnungszentrum Emmendingen betreibt eigene Zertifizierungsstellen (CAs: Certification Authorities). Dieses Dokument ist die CP (Certificate Policy) der CAs des Abrechnungszentrum Emmendingen. Es beschreibt Spezifikationen, Prozesse und technische und organisatorische Sicherheitsmaßnahmen der CAs für die Ausstellung von Zertifikaten.

Diesem Dokument zu Grunde liegen die Empfehlungen von RFC 3647.

Damit die Authentizität und die Vertraulichkeit bei der Kommunikation der einzelnen Teilnehmer untereinander gesichert ist, wird eine Public Key Infrastruktur (PKI) etabliert. Technisch wird der Authentizitätsnachweis der Schlüssel dabei über digitale X.509-Zertifikate aus der PKI realisiert.

Die Systemarchitektur der PKI wird in die folgenden drei Hierarchiestufen unterteilt:

- Die **Root-CA**, welche den hoheitlichen Vertrauensanker der PKI darstellt.
- Die **Sub-CAs**, die zur Zertifizierung von Endnutzerschlüsseln dienen.
- Die **Endnutzer**, welche die untere Ebene der PKI bilden und ihre Zertifikate zur Kommunikation miteinander und insbesondere zum Aufbau gesicherter Verbindungen nutzen.

Die in der PKI Policy verwendeten Inhalte werden dem [RFC 2119] entsprechend mit folgenden deutschen Schlüsselworten beschrieben:

- **MUSS** bedeutet, dass es sich um eine normative Anforderung handelt.
- **DARF NICHT / DARF KEIN** bezeichnet den normativen Ausschluss einer Eigenschaft.
- **SOLLTE / EMPFOHLEN** beschreibt eine dringende Empfehlung. Es müssen triftige Gründe vorliegen, um die Empfehlung nicht umzusetzen, wobei die Entscheidung dazu unter Abwägung aller Auswirkungen auf den jeweiligen Betrieb getroffen werden muss.
- **SOLLTE NICHT / SOLLTE KEIN** kennzeichnet die dringende Empfehlung, eine Eigenschaft auszuschließen.
- **KANN / DARF** bedeutet, dass die Eigenschaften fakultativ oder optional sind.

Die Kapitel der PKI Policy sind grundsätzlich als normativ anzusehen. Informative Kapitel werden explizit am Anfang gekennzeichnet.

1.1 Überblick

Das Dokument richtet sich sowohl an die Betreiber der Root- oder einer Sub-CA als auch an die weiteren Teilnehmer und ist in Anlehnung an [RFC 3647] strukturiert und definiert. Nachfolgend wird die Struktur erläutert:

Nach der Einleitung werden zunächst die Indexe beschrieben. Hierunter fallen, neben der Darstellung der Verzeichnisse, Details dazu, welche Informationen durch die Root- und die Sub-CAs zu veröffentlichen sind, die Häufigkeit der Veröffentlichung sowie Zugriffskontrollen auf diese Komponenten.

Die Verantwortlichkeit für die PKI Policy sowie den Betrieb der Root obliegt dem Abrechnungszentrum Emmendingen als Inhaber der Wurzelzertifikate der PKI.

Das Abrechnungszentrum Emmendingen behält sich vor, komplette Aufgaben oder Teilaufgaben von beauftragten Unternehmen ausführen zu lassen.

1.2 Name und Identifizierung des Dokuments

Dieses Dokument ist die Certificate Policy (CP) der Abrechnungszentrum Emmendingen PKI (PKI) und kann über die folgenden Informationen identifiziert werden.

Identifikator	Wert
Titel	Zertifizierungsrichtlinie (Certificate Policy) Abrechnungszentrum Emmendingen
Version	4.0

Tabelle 1: Identifikation des Dokuments

1.3 PKI-Teilnehmer

In diesem Unterkapitel werden die Teilnehmer (Zertifizierungsstellen, Registrierungsstellen, Zertifikatsnehmer und Zertifikatsnutzer) der PKI aufgeführt. Die nachfolgende Tabelle zeigt einen Überblick über die PKI-Teilnehmer:

Instanz der PKI	Zertifizierungsstelle	Zertifikatsnehmer	Zertifikatsnutzer
Root-CA	X	X	X
Sub-CA	X	X	X
Zertifikat (Server)		X	X
Zertifikat (Client)			X

Tabelle 2 Übersicht der PKI-Teilnehmer

1.3.1 Zertifizierungsstellen

In diesem Unterkapitel werden nachfolgend die CAs der PKI beschrieben.

Nachfolgend werden die unterschiedlichen Bestandteile der CAs der PKI erläutert

1.3.1.1 ROOT-CA

Die Root-CA bildet den nationalen Vertrauensanker der PKI für die Berechtigung zur Ausstellung und Nutzung der Zertifikate und ist der Herausgeber dieser PKI Policy.

1.3.1.2 Sub-CA

Eine Sub-CA ist eine Instanz, welche von der Root-CA zur Ausstellung von Zertifikaten autorisiert wird und Zertifikate für die Endnutzer ausstellt.

Der Betrieb einer Sub-CA kann auf unterschiedliche Arten erfolgen, die in der internen PKI-Dokumentation des Abrechnungszentrum Emmendingen beschrieben sind. Diese PKI Policy definiert Sicherheitsvorgaben für den Betrieb einer Sub-CA.

1.3.2 Registrierungsstellen

Registrierungsstellen (Registration Authority, RA) führen vor der Ausstellung eines Zertifikats die zweifelsfreie Identifizierung des Antragstellers und die Authentifizierung der PKI-Rolle und der Identitätsdaten der ausführenden Personen für den Antragssteller durch.

Die Registrierungsstelle der Root CA bildet das Abrechnungszentrum Emmendingen. Diese ist für die Bearbeitung der initialen Registrierungen sowie der Wiederholungsanträge der Sub-CA zuständig.

Eine Sub-CA verfügt unter Umständen jeweils über eigene Registrierungsstellen innerhalb des Abrechnungszentrums Emmendingen (RA der Sub-CA). Diese sind für die initialen Registrierungen sowie die Wiederholungsanträge der Endnutzer zuständig. Die Grundlage für die Prozesse der RA bilden die Vorgaben dieser PKI Policy.

1.3.3 Zertifikatsnehmer

Die nachfolgend beschriebenen PKI-Teilnehmer werden auch als Endnutzer oder Zertifikatsinhaber bezeichnet, da diese ihre Zertifikate nicht zur Ausstellung von Zertifikaten, sondern ausschließlich zur Absicherung der Kommunikation verwenden.

1.3.3.1 Externer Zertifizierungsteilnehmer

Ein externer Zertifizierungsteilnehmer (EZT) erhält von einer Sub-CA der PKI Zertifikate, mit denen dieser insbesondere mit den Systemen des Abrechnungszentrum Emmendingen sicher kommunizieren kann. Überdies kann der Datenaustausch mit den anderen Teilnehmern der PKI abgesichert werden.

1.3.3.2 Zertifikatsnutzer

Zertifikatsnutzer im Sinne dieser PKI Policy sind alle natürlichen und juristischen Personen bzw. technischen Komponenten, die Zertifikate aus der PKI für die Erledigung von Geschäftsprozessen/Aufgaben verwenden.

1.3.4 Andere Teilnehmer

Teilnehmer (wie z.B. Endverbraucher), welche keine Verpflichtung im Rahmen dieser PKI Policy eingegangen sind, sind nicht Bestandteil der PKI Policy und werden daher nicht berücksichtigt. Ergeben sich beispielsweise durch die internationale Anbindung anderer Infrastrukturen weitere Teilnehmer, so MÜSSEN sowohl deren PKI-Rollen als auch deren Interaktionen den Sicherheitsanforderungen aus dieser PKI Policy entsprechen.

1.4 Verwendung von Zertifikaten

In diesem Abschnitt wird die erlaubte und verbotene Verwendung von Zertifikaten in der PKI definiert.

1.4.1 Erlaubte Verwendung von Zertifikaten

Jeder PKI-Teilnehmer benötigt für die Ausübung seiner PKI-Rolle entsprechende Zertifikate aus der PKI. Ein Teilnehmer KANN über mehrere Zertifikate bzw. Zertifikatstriple verfügen.

Das Schlüsselmaterial der PKI-Teilnehmer kann zur Authentisierung, zur Verschlüsselung und zur Erstellung von elektronischen Signaturen eingesetzt werden.

In den nachfolgenden Tabellen werden alle Zertifikate den unterschiedlichen PKI-Teilnehmern zugeordnet und der entsprechende Verwendungszweck erläutert.

Root-CA:

Zertifikat der Root-CA	Signiert durch	Verwendungszweck
C(Root)	Privater Schlüssel zu C(Root)	Vertrauensanker der PKI: Der öffentliche Schlüssel aus dem Zertifikat wird zur Überprüfung der Signatur von nachgeordneten Zertifikaten benötigt. Der zugehörige private Schlüssel wird für die Signatur von Sub-CA-, sowie von C(Root)-, Link-C(Root)-, C_{CRL-S}(Root)- und C_{TLS-S}(Root)-Zertifikaten verwendet.
Link-C(Root)	Privater Schlüssel zu C(Root)	Das Link-C(Root)-Zertifikat dient zur Echtheitsprüfung eines neuen C(Root). Mit diesem Zertifikat kann das aktuelle C(Root) mit dem vorherigen C(Root) verifiziert werden (gilt nicht für die initiale Root, da dieser Prozess erst ab dem ersten „Folgezertifikat“ genutzt werden kann).
C_{CRL-S}(Root)	Privater Schlüssel zu C(Root)	Mit Hilfe dieses Zertifikats kann die Signatur der Sperrliste (Root-CA-CRL) verifiziert werden. Der zugehörige private Schlüssel wird für die Signatur der Root-CA-CRL verwendet.
C_{TLS-S}(Root)	Privater Schlüssel zu C(Root)	Dieses Zertifikat wird bei der Verifikation der C_{TLS}(Root)-Zertifikate und der Sperrliste (Root-TLS-CRL) verwendet. Der zugehörige private Schlüssel wird für die Signatur von $C_{TLS,Root}$(Sub-CA)- Zertifikaten, C_{TLS}(Root)-Zertifikaten und der Root-TLS-CRL verwendet.
C_{TLS}(Root)	Privater Schlüssel zu C_{TLS-S}(Root)	Diese Zertifikate werden beim Aufbau des TLS-Kommunikationskanals zwischen Root und anderen Systemen eingesetzt.

Tabelle 3 Zertifikate der Root-CA

SUB-CA:

Zertifikat einer Sub-CA	Signiert durch	Verwendungszweck
C(Sub-CA)	Privater Schlüssel zu C(Root)	Der öffentliche Schlüssel aus dem Zertifikat wird zur Überprüfung der Signatur von nachgeordneten Zertifikaten benötigt, welche mit dem zum Zertifikat passenden privaten Schlüssel signiert wurden. Der zugehörige private Schlüssel wird für die Signatur von Zertifikaten und der Sperrliste der Sub-CA verwendet.
$C_{TLS,Root}$(Sub- CA)	Privater Schlüssel zu C_{TLS-S}(Root)	Diese Zertifikate werden beim Aufbau des TLS-Kommunikationskanals zwischen Sub-CA und der Root für das Zertifikatsmanagement eingesetzt.
C_{TLS}(Sub- CA)	Privater Schlüssel zu C(Sub-CA)	Diese Zertifikate werden beim Aufbau des TLS-Kommunikationskanals zwischen Sub-CA und anderen

Tabelle 4 Zertifikate der Sub-CA

Zertifikate der Zertifikatsnehmer (außer Root-CA und Sub-CA):

Zertifikat eines Zertifikats-nehmers	Signiert durch	Verwendungszweck
C_{TLS}(Cert)	Privater Schlüssel zu C(Cert)	Zertifikat des entsprechenden Endnutzers zur Authentisierung beim Kommunikationspartner und zum Aufbau einer TLS-Verbindung.
C_{Enc}(Cert)	Privater Schlüssel zu C(Cert)	Zertifikat des entsprechenden Endnutzers zur Authentisierung beim Kommunikationspartner und zum Aufbau einer TLS-Verbindung.
C_{Sig}(Cert)	Privater Schlüssel zu C(Cert)	Zertifikat zur Verifikation von Inhaltsdatensignaturen des entsprechenden Endnutzers.

Tabelle 5 Zertifikate der Zertifikatsnehmer

Andere Zertifikate (nicht von der PKI bereitgestellt):

Für die Kommunikation der Ansprechpartner (ASP) in den unterschiedlichen Ebenen ist der Informationsaustausch mittels verschlüsselter und signierter E-Mails oder der Bereitstellung über sichere Datenkanäle vorgesehen.

1.4.2 Verbotene Verwendung von Zertifikaten

Die Zertifikate MÜSSEN gemäß ihrem Verwendungszweck eingesetzt werden.

1.5 Administration der PKI Policy

Die für dieses Dokument verantwortliche Organisation ist das Abrechnungszentrum Emmendingen (ARZ). Das ARZ kann über folgende Adresse kontaktiert werden:

Organisation	Abrechnungszentrum Emmendingen
Adresse	An der B3 Haus Nr. 6 79312 Emmendingen
Fax	+49 7641-9201-777
E-Mail	zertifikat@arz-emmendingen.de
Webseite	http://pki.arz-emmendingen.de/

Tabelle 6 Kontaktadresse

1.5.1 Pflege der PKI Policy

Jede aktualisierte Version der PKI Policy wird den Anwendern unverzüglich über die angegebene Internetseite zur Verfügung gestellt.

Überdies wird über die Internetseite ein Changelog bereitgestellt, um Klarstellungen oder kleinere Änderungen zur PKI Policy kurzfristig veröffentlichen zu können.

1.5.2 Zuständigkeit für das Dokument

Zuständig für die Erweiterung und oder die nachträglichen Änderungen dieser PKI Policy ist die Root CA.

1.5.3 Ansprechpartner / Kontaktperson

Siehe Tabelle 6.

1.5.4 Zuständiger für die Anerkennung eines CPS

Ein CPS (Certificate Practice Statement) einer CA ist ein Dokument, welches beschreibt, wie die Anforderungen dieser Zertifizierungsrichtlinie umgesetzt werden und ist Bestandteil der internen betrieblichen Dokumentation des Abrechnungszentrums Emmendingen.

1.5.5 CPS-Aufnahmeverfahren

Ein CPS der PKI MUSS konform zu dieser CP sein.

2 Verantwortlichkeit für Veröffentlichungen und Verzeichnisse

2.1 Sperrliste

Es MUSS von der Root-CA und allen Sub-CAs jeweils eine auf deren Verantwortungsbereich beschränkte Sperrliste erzeugt werden, in der alle gesperrten Zertifikate während ihres Gültigkeitszeitraums aufgeführt sind.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

2.2.1 Veröffentlichungen der Root-CA

Die Root-CA MUSS über ihre Webseiten folgende Informationen bereitstellen:

- Kontaktdaten der Root
- Diese PKI Policy
- Die aktuellen Zertifikate der Root-CA inklusive der SHA256 Hashs
- Parameter zur Einrichtung eines Zugriffs auf die Sperrliste
- Beschreibung des Antragsverfahrens für eine Sub-CA Berechtigung
- Formular zur Beantragung einer Sub-CA Berechtigung
- Informationen zu den zu erstellenden Sub-CA Zertifikatsrequests
- Informationen zum Sperrprozess für Sub-CA Zertifikate
- Changelogs zur PKI Policy

2.2.2 Veröffentlichungen der Sub-CA

Eine Sub-CA SOLLTE NICHT über eine Web-Seite verfügen, jedoch folgende Informationen beinhalten:

- Kontaktdaten der Sub-CA
- Die aktuellen Zertifikate der Sub-CA inklusive der SHA256 Hashs. Das Format, in dem die Zertifikate und Hashs vorliegen, muss angegeben werden.
- Parameter zur Einrichtung eines Zugriffs auf die Sperrliste
- Certificate Policy der Sub-CA mit folgenden Mindestanforderungen:
    - Die CP MUSS die Anforderungen und somit die Einhaltung dieser PKI Policy bestätigen.
    - Die CP MUSS die für die Bereitstellung und Verwaltung der Zertifikate notwendigen Prozesse grundsätzlich beschreiben. Diesbezüglich kann auch auf die entsprechenden Stellen in dieser PKI Policy verwiesen werden.
    - Die CP MUSS die für den Betrieb verantwortlichen Bereiche / Ansprechpartner benennen. Die folgenden weiteren Informationen SOLLTEN bereitgestellt werden:
- Beschreibung des Antragsverfahrens von Zertifikaten unterhalb dieser Sub-CA
- Formulare zur Beantragung von Zertifikaten
- Informationen zu den zu erstellenden jeweiligen Zertifikatsrequests

- Informationen zum Sperrprozess von Zertifikaten

2.3 Zeitpunkt und Häufigkeit der Veröffentlichungen

Alle Zertifikatskomplementärinformationen (z.B. Sperrlisten) innerhalb der PKI MÜSSEN unmittelbar nach der Ausstellung veröffentlicht werden.

Eine Sperrung wird nach Durchführung durch eine Veröffentlichung in der jeweiligen Sperrliste der Root-CA / Sub-CA als solche wirksam. Eine Aufnahme in die Sperrliste sowie deren Veröffentlichung erfolgt gemäß den in der Tabelle 9 festgelegten Zeiten.

Nach Ablauf der im Zertifikat eingetragene Gültigkeit MUSS der Eintrag aus der Sperrliste entfernt werden.

3 Identifizierung und Authentifizierung

Dieses Kapitel beschreibt die durchzuführenden Prozeduren, um die Identität und die Berechtigung eines Antragstellers vor dem Ausstellen eines Zertifikats festzustellen.

3.1 Regeln für die Namensgebung

Hinsichtlich des Namensschemas MUSS der Bezeichner (common name (CN)) eines Zertifikats der PKI dem Profil gemäß Anhang A entsprechen.

3.1.1 Arten von Namen Regelungen von Ausnahmen

Die Inhalte für die Identifikation des Zertifikatsinhabers (Subject) bzw. des Zertifikatsherausgebers (Issuer) der verschiedenen Zertifikate der PKI werden im Anhang A spezifiziert.

3.1.2 Notwendigkeit für aussagefähige Namen

Die Angaben der Zertifikatsinhaber MÜSSEN in die Zertifikate aufgenommen werden.

3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern

Der Zertifikatsnehmer SOLLTE NICHT anonym sein oder Pseudonyme verwenden.

3.1.4 Eindeutigkeit von Namen

Die Angaben der Zertifikatsinhaber MÜSSEN in die Zertifikate aufgenommen werden.

Eine Namensgleichheit (gleicher CN bei unterschiedlichem Zertifikatsnehmer) SOLLTE durch die CAs verhindert werden, entsprechend DARF eine CA einen CN NICHT mehrfach vergeben.

Bei der Ausstellung von Zertifikaten ist ein Abgleich hinsichtlich der Eindeutigkeit von Namen zwischen den Sub-CA‘s nicht erforderlich.

Sollten zwei oder mehr Zertifikatsnehmer von einer CA den gleichen CN besitzen, besteht ein Konflikt der gelöst werden MUSS. Es behält der Teilnehmer seinen CN, der zuerst sein erstes Zertifikat mit diesem CN erhalten hat. Der oder die anderen Zertifikatsnehmer MÜSSEN sich ein neues Zertifikat mit einem anderem CN ausstellen lassen, um weiterhin an der PKI teilnehmen zu DÜRFEN.

3.1.5 Anerkennung, Authentifizierung und die Rolle von Markennamen

Die Eintragung der Firmennamen MÜSSEN auf Basis der Identität, die im Rahmen der initialen Überprüfung in das erste Zertifikat übernommen wurde, erfolgen.

3.2 Initiale Überprüfung zur Teilnahme an der PKI

Dieser Abschnitt enthält Informationen über die Identifizierungsprozeduren, d. h. die Prüfung der natürlichen Person als Vertreter des Unternehmens, und die Authentifizierungsprozeduren, d.h. die Prüfung der Anforderung und der Qualifikation

des Unternehmens, für den initialen Zertifikatsantrag der unterschiedlichen Zertifikatsnehmer.

Auf der **Root-Ebene** wird das Ausstellen des selbstsignierten C(Root) sowie der $C_{CRL\text{-}S}$(Root), $C_{TLS\text{-}S}$(Root), C_{TLS}(Root) und Link-C(Root)-Zertifikate nicht betrachtet, da die Registrierungsstelle und der Betrieb für die Root eine organisatorische Einheit bilden. Somit ist eine Identifizierung und Authentifizierung auf Root-Ebene gegeben.

3.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

Zum Nachweis des Besitzes des privaten Schlüssels MUSS ein Zertifikatsrequest eine sogenannte innere Signatur beinhalten.

Hierdurch MUSS bei der Antragsprüfung durch Verifikation der inneren Signatur mit dem im Zertifikatsrequest enthaltenen zugehörigen öffentlichen Schlüssel durch die CA geprüft werden, dass der Antragsteller im Besitz des privaten Schlüssels ist.

3.2.2 Authentifizierung von Organisationszugehörigkeiten

Die nachfolgenden Organisationen DÜRFEN innerhalb der PKI Zertifikatsanträge stellen.

3.2.2.1 Sub-CA

Zur initialen Autorisierung einer neuen Sub-CA MÜSSEN das Unternehmen authentifiziert und mindestens zwei bevollmächtigte Vertreter des Betreibers persönlich bei dem Betreiber der Root-CA identifiziert und authentifiziert werden.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zum Aufbau einer Sub-CA mit folgenden Daten bzw. beigefügten Informationen
    - Name der Firma bzw. der Institution
    - Anschrift des Unternehmens bzw. der Institution
    - Unternehmensnachweis (z.B. aktueller Auszug aus dem Handelsregister) oder Nachweis der Institution (durch ein entsprechendes Siegel der Institution)
    - Aussage zum Typ der geplanten Sub-CA (unternehmensintern oder -übergreifend)
    - Bei der Beauftragung eines Dienstleisters für den Betrieb einer Sub-CA MUSS der Betreiber eine Bestätigung des beauftragenden Unternehmens vorlegen, welches den Dienstleister zur Beantragung und zum Betrieb der Sub-CA berechtigt.
    - Kontaktdaten der Ansprechpartner (unter Beachtung einer Vertreterregelung)
    - Bestätigung der Geschäftsführung des Unternehmens bzw. der Leitung der Institution, in der der Ver treter des Betreibers berechtigt wird, den Antrag für die Sub-CA zu stellen und in der Sache dazu verbindliche Aussagen und Angaben zu machen.
- Certificate Policy der Sub-CA

- Nachweis zum sicheren Betrieb der Sub-CA gemäß den Vorgaben zu den Anforderungen für die Teilnahme an der PKI.
- Bestätigung der erfolgreichen Testteilnahme

Vor der initialen Identifizierung und Authentifizierung MUSS der Betrieb der Sub-CA im Rahmen einer Testteilnahme erfolgreich erprobt worden sein. In diesem Test MÜSSEN mindestens eine Zertifikatsbeantragung und eine Zertifikatssperrung erfolgreich durchlaufen werden. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der Test- Root-CA per signierter E-Mail bestätigt.

Die Hashwerte (SHA 256) der initialen Zertifikatsrequests für das Signatur- (C(Sub-CA)) und das TLS-Zertifikat ($C_{TLS,Root}$(Sub-CA)) der Sub-CA MÜSSEN in gedruckter Form inklusive der Information zum Format der Darstellung mit der Bestätigung durch die Unterschrift des Bevollmächtigten vorgelegt werden. Der Hashwert wird dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequests-Paket enthält, und als base64-codierter Ausdruck in diesem Prozess verwendet.

Die eigentlichen Zertifikatsrequests KÖNNEN zusätzlich im Rahmen dieses Termins als Dateien übergeben werden.

Es wird EMPFOHLEN, die Zertifikatsrequests dem Root-Betreiber vorab zuzusenden, so dass vor dem Termin eine Überprüfung auf Konformität erfolgen kann.

3.2.2.2 Client-/Server-Zertifikat

Zur Aufnahme eines neuen Client-/Server-Zertifikat in die PKI MUSS durch den Sub-CA-Betreiber eine Authentifikation des Unternehmens erfolgen.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zur Ausgabe eines Zertifikats mit folgenden Daten bzw. beigefügten Informationen
    - Name der Firma bzw. der Institution
    - Anschrift des Unternehmens bzw. der Institution
    - Unternehmensnachweis (z.B. aktueller Auszug aus dem Handelsregister) oder Nachweis der Institution (durch ein entsprechendes Siegel der Institution)
    - Kontaktdaten der Ansprechpartner (unter Beachtung einer Vertreterregelung)
    - Bei der Beauftragung eines Dienstleisters für den Betrieb des EZT MUSS der Betreiber eine Bestätigung des Unternehmens vorlegen, die den Dienstleister zur Beantragung und zum Betrieb für das Zertifikat berechtigt.
    - Bestätigung der Geschäftsführung des Unternehmens bzw. der stellvertretenden Leitung der Institution, in der der Vertreter des Betreibers berechtigt wird, den Antrag für das Zertifikat zu stellen

und in der Sache dazu verbindliche Aussagen und Angaben zu machen.

- Erklärung zur Nutzung des Client-/Server-Zertifikats
    - Aus der Erklärung MUSS nachvollzogen werden können, welche Funktionen und Aufgaben ein Zertifikat wahrnehmen will.
- Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser PKI Policy
    - Es MUSS eine Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser PKI Policy mit einreicht werden.
    - Es MUSS den Nachweis des sicheren Betriebs gemäß den Vorgaben zu den Anforderungen für die Teilnahme an der PKI erbracht werden.

Vor der Wirkbetriebsaufnahme MÜSSEN die Prozesse zum Zertifikatsmanagement (insbesondere Registrierung, Zertifikatsbeantragung, -erneuerung, -sperrung) der jeweiligen Sub-CA erfolgreich durchgeführt worden sein. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der Sub-CA per E-Mail bestätigt.

3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikats- Antragstellers

Ein Zertifikatsrequest DARF NICHT von einer Einzelperson (natürliche Person), sondern MUSS von einer Organisation (juristische Person) gestellt werden.

3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Die Registrierungsstelle MUSS die Angaben zum Zertifikatsnehmer im Zertifikatsrequest gegen die eingereichten Unterlagen auf Korrektheit prüfen.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Siehe Abschnitt Client-/Server-Zertifikat.

3.2.6 Kriterien für den Einsatz interoperierender Systeme/Einheiten

Aktuell sind keine Kriterien definiert.

3.2.7 Aktualisierung / Anpassung der Registrierungsinformationen der Teilnehmer

Jeder Teilnehmer an der PKI MUSS der Root-CA bzw. der entsprechenden Sub-CA unverzüglich mitteilen, falls sich Änderungen bzgl. seiner Registrierungsdaten ergeben. Ergänzend SOLLTE die Root-CA sowie jede Sub-CA regelmäßig (z.B. jährliches Intervall) über die Ansprechpartner bei den Klienten anfragen, ob Änderungen an den Registrierungsdaten vorliegen.

3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (Routinemäßiger Folgeantrag)

Nach der initialen Zertifikatsausstellung erfolgen sogenannte Folgeanträge. Diese MÜSSEN ebenso wie die initialen Zertifikatsanträge zweifelsfrei von der jeweiligen CA identifiziert und authentisiert werden.

Bei einer Schlüsselerneuerung (Folgeantrag zu einem bestehenden Zertifikat) ist zu beachten, dass von dem Antragsteller immer ein neuer Schlüssel erstellt werden MUSS.

Ein Zertifikatsinhaber ist dafür verantwortlich, rechtzeitig, d.h. vor dem Ablauf aller Zertifikate, neue Zertifikate zu beantragen. Der Zeitraum MUSS so gewählt werden, dass die neuen Zertifikate rechtzeitig in die Systeme eingebracht werden können, so dass der Betrieb ohne Beeinträchtigungen fortgeführt werden kann.

Der Antragsteller besitzt einen privaten Schlüssel des dem Betreiber zugeordneten TLS-Zertifikats, mit dem die Absicherung des Kommunikationskanals durchgeführt wird. Das Zertifikat zu diesem Schlüssel darf weder gesperrt noch abgelaufen sein. Der zu übermittelnde Zertifikatsrequest (unabhängig von dem Zertifikats- typ) bzw. das Zertifikatsrequest-Paket ist mit dem zuletzt gültigen Signaturschlüssel signiert worden, und das zugehörige Zertifikat ist noch gültig und nicht gesperrt.

Nach der erfolgreichen Prüfung eines routinemäßigen Folgeantrags erfolgt die Ausstellung des beantragten Zertifikats.

3.4 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (Nicht routinemäßiger Folgeantrag)

3.4.1 Allgemein

Um einen nicht routinemäßigen Folgeantrag handelt es sich, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

- Der Antragssteller besitzt kein gültiges TLS-Zertifikat für die Beantragung.
- Der Zertifikatsrequest ist nicht mit der gültigen Signatur des vorherigen Signaturschlüssels versehen.

Entsprechend ist eine der beiden Absicherungen eines Folgeantrags nicht gegeben, daher kann der vorher beschriebene Regelprozess (routinemäßiger Folgeantrag) nicht genutzt werden. Die weitere Vorgehensweise unterscheidet sich anhand der dem Antragsteller zu diesem Zeitpunkt noch zur Verfügung stehenden Sicherheitsmechanismen.

Beide Absicherungen fehlen

Sind beide Absicherungen (gültiges TLS-Zertifikat und gültige äußere Signatur) nicht gegeben, MUSS ein neues initiales Zertifikatsrequest-Paket im Rahmen einer erneuten initialen Identifizierung des PKI-Teilnehmers werden.

Ungültiges TLS-Zertifikat

Kann keine Authentifikation mittels des TLS-Zertifikats gegenüber der CA mehr erfolgen, MUSS die Übermittlung des Zertifikatsrequests über einen anderen gesicherten Kanal (z.B. eine verschlüsselte und signierte E-Mail des benannten ASP des Zertifikatsnehmers) durchgeführt werden. Bei der Beantragung MUSS immer auch ein neues TLS-Zertifikat beantragt werden. Dies ist auf Endnutzer-Ebene automatisch gegeben, da hier immer ein Zertifikatstripel beantragt wird. Durch die

Erneuerung des TLS-Zertifikats müssen dann wieder routinemäßige Folgeanträge über den TLS-abgesicherten Webservice gestellt werden können. Die Beantragung von Zertifikaten MUSS, unabhängig vom Kommunikationskanal, immer über Zertifikatsrequest-Pakete erfolgen.

Ungültige „Äußere Signatur“ (z.B. ungültiges Signatur-Zertifikat)

Kann die Autorisation des Zertifikatsrequests nicht mehr über Signatur mit einem vorherigen, noch gültigen Signaturschlüssel erfolgen, MUSS ein neues initiales Zertifikatsrequest-Paket (identisch mit dem Zertifikatsrequest bei der ersten Beantragung der Zertifikate) übermittelt werden.

Verfügt der PKI-Teilnehmer noch über ein gültiges TLS-Zertifikat MUSS das neue initiale Zertifikatsrequest-Paket hiermit signiert und über einen gesicherten Kanal an die CA übermittelt werden.

Zusätzlich wird ebenfalls über einen gesicherten Kanal (z.B. eine verschlüsselte und signierte E-Mail des benannten ASP des Zertifikatsnehmers) der Hashwert des Zertifikats-Pakets zum Abgleich und zur Autorisation zugesendet. Die Hashwerte (SHA 256) werden dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket enthält, und als base64-codierter Ausdruck in einer Datei versendet wird.

Nach einem positiven Abgleich des Hashwertes durch die Mitarbeiter der jeweiligen CA werden die Zertifikate zur Verfügung gestellt. Der erfolgreiche Abgleich des Hashwertes MUSS durch die CA mit Angabe der beteiligten Personen dokumentiert werden.

3.4.2 Schlüsselerneuerung nach Sperrungen

Das weitere Vorgehen zur Identifizierung und Authentifizierung eines PKI-Teilnehmers nach einer Sperrung ist davon abhängig, welche seiner Zertifikate von der Sperrung betroffen sind. Der PKI-Teilnehmer MUSS auf Basis der ihm zur Verfügung stehenden gültigen Zertifikate, einen Folgeantrag gemäß dem vorangegangenen Unterkapitel stellen, um seine gesperrten Zertifikate durch neue gültige Zertifikate zu ersetzen. Ein Endnutzer MUSS immer ein neues Zertifikatstripel beantragen, wenn eines seiner Zertifikate gesperrt wurde.

3.5 Identifizierung und Authentifizierung von Anträgen auf Sperrung

Die Sperrung eines Zertifikates kann von den folgenden Beteiligten initiiert werden:

- dem Zertifikatsinhaber oder
- der Root-CA bzw. der ausstellenden Sub-CA.

Bei einer Sperrung MÜSSEN dafür folgende Informationen an die Root- bzw. die Sub-CA von einem benannten Ansprechpartner mittels signierter E-Mail oder einem vergleichbar abgesicherten Kommunikationskanal übermittelt werden:

- Zertifikatstyp
- Ausstellende Sub-CA bzw. Root-CA

- Zertifikatsnummer (Der Wert des Felds “SerialNumber“ des Zertifikats)
- Sperrgrund
- Zeitpunkt, ab dem das Zertifikat als unsicher/gesperrt einzustufen ist (optional, nur wenn genauer Zeit - punkt bekannt ist)

3.5.1 Initiative des Zertifikatsinhabers

Der Zertifikatsinhaber stellt im Rahmen des Betriebs einen Grund zur Sperrung des Zertifikats fest. Diese Gründe sind insbesondere

- eine Änderung der Zertifikatsdaten,
- eine Schlüsselkompromittierung oder
- die Einstellung des Betriebs.

Der benannte Ansprechpartner sendet in diesem Fall eine E-Mail an den Betreiber der CA. Dieser prüft die Authentizität der Information und sperrt das Zertifikat.

Die Sperrung des jeweiligen Zertifikats MUSS über die Sperrliste der zuständigen CA veröffentlicht werden und der Zertifikatsinhaber MUSS über den abgeschlossenen Sperrprozess per E-Mail informiert werden.

Die Sub-CA KANN zusätzliche Verfahren zur Initiierung einer Sperrung anbieten, sofern dieser über eine authentisierte und integre Kommunikationsschnittstelle verfügt. Das Sicherheitsniveau muss mit dem der Webservice-Schnittstelle vergleichbar sein. Diese optionalen Verfahren MÜSSEN in der Certificate Policy der Sub-CA beschrieben werden.

3.5.2 Initiative des Betreibers der Certificate Authority

Der Betreiber der CA hat die Aufgabe, bei erkannten Schwachstellen alle Tätigkeiten durchzuführen, welche die Integrität und Sicherheit der PKI sicherstellen. Die Einleitung weiterer Schritte ist ggf. in Absprache mit der Root vorzunehmen. Mögliche Gründe sind beispielsweise

- ein erkannter Verstoß gegen Betriebsauflagen,
- erkannte (erhebliche) Schwächen in der eingesetzten Kryptographie oder Kryptoimplementierung,
- Änderungen in den zentralen Vorgaben,
- Änderung der Zertifikatsdaten (z.B. des Organisationsnamens),
- eine erkannte Schlüsselkompromittierung oder
- die Einstellung des Betriebs bzw. die Außerbetriebnahme der betroffenen Komponente.

Sperrungen von Zertifikaten mit systemrelevanter Bedeutung (Sub-CA) MÜSSEN in Abstimmung mit der Root erfolgen.

Eine Sperrung des jeweiligen Zertifikats MUSS über die Sperrliste der CA veröffentlicht werden. Der Zertifikatsinhaber sowie die Root MÜSSEN über den abgeschlossenen Sperrprozess in - formiert werden.

4 Betriebsanforderungen für den Zertifikatslebenszyklus

In diesem Kapitel werden die Prozeduren und Verantwortlichkeiten für den Lebenszyklus von Zertifikaten definiert. Dies umfasst insbesondere folgende Bereiche:

- Zertifikatsbeantragung (initiale Beantragung und Folgeantrag),
- Verarbeitung von Zertifikatsanträgen und
- Zertifikatsausstellung.

Innerhalb der Prozesse des Zertifikatslebenszyklus SOLLTE die relevante personenbezogene Kommunikation verschlüsselt werden.

4.1 Zertifikatsantrag

In den folgenden Unterkapiteln wird definiert, wer ein Zertifikat in der PKI beantragen darf und welche Stelle für die Bearbeitung des Zertifikatsantrags verantwortlich ist.

4.1.1 Wer kann einen Zertifikatsantrag stellen?

Ein Zertifikatsrequest darf ausschließlich von einer Organisation gestellt werden. Befugte Organisationen MÜSSEN identifiziert werden.

Ein Endnutzer KANN sofern erforderlich weitere Zertifikate bzw. Zertifikatstriple für sich beantragen (z.B. für Lastmanagement oder Ausfallsicherheit).

Der Zertifikatsrequest MUSS als Folgeantrag unter Nutzung der vorhandenen Zertifikate bei der Root-CA oder einer Sub-CA gestellt werden.

Die weiteren Zertifikate/Zertifikatstriple MÜSSEN eindeutig gekennzeichnet werden. Die Eindeutigkeit von Zertifikaten erfolgt aus der Kombination von Common Name, der Sequenznummer im Subject-DN, der Seriennummer des Zertifikats und dem Issuer-DN (Herausgeber/CA).

4.1.2 Beantragungsprozess und Zuständigkeiten

Für die Bearbeitung eines Zertifikatsantrags ist die Registration Authority (RA) der jeweiligen CA verantwortlich.

4.2 Verarbeitung von initialen Zertifikatsanträgen

4.2.1 Durchführung der Identifizierung und Authentifizierung

Der Zertifikatsnehmer übergibt durch seinen benannten Ansprechpartner, je nach Definition, die Unterlagen und Nachweise für die initiale Zertifikatsbeantragung an die RA einer CA.

Die RA-Mitarbeiter dieser CA prüfen die eingereichten Dokumente / Nachweise. Sollten die Unterlagen / Nachweise nicht vollständig oder fehlerhaft sein, informieren diese den ASP des Zertifikatsnehmers und fordern ihn zur Nachlieferung auf.

Sollte einer der benannten und identifizierten Mitarbeiter ausscheiden, MUSS sich mindestens ein neuer Vertreter im Rahmen eines persönlichen Termins bei der CA identifizieren lassen. Die Benennung des neuen Vertreters bzw. der neuen Vertreter sowie die Information über das Ausscheiden des bisherigen Vertreters MUSS von einem der benannten Ansprechpartner des Teilnehmers bestätigt werden.

4.2.2 Annahme oder Ablehnung von initialen Zertifikatsanträgen

Die vorliegenden bzw. nachgelieferten Unterlagen / Nachweise werden von den RA-Mitarbeitern gegen die Vorgaben aus der PKI Policy der jeweiligen Certification Authority geprüft.

Im Positivfall wird der Zertifikatsantrag formell freigegeben und der benannte Ansprechpartner per E-Mail darüber informiert.

Durch die RA MÜSSEN im Rahmen der Prüfung auch der vorliegende Zertifikatsrequest für die initialen Zertifikate formal und die Übereinstimmung der gedruckten Hashwerte in den Unterlagen mit denen der Zertifikatsrequests überprüft werden.

Im Negativfall MUSS der Zertifikatsantrag formell abgelehnt und der benannte Ansprechpartner per E-Mail über die Ablehnung (incl. entsprechender Begründung) informiert werden. Der Beantragungsprozess ist mit diesem Schritt beendet und MUSS durch den Zertifikatsnehmer ggf. neu initiiert werden.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Die in den nachfolgenden Abschnitten aufgeführten Zeiten sind als Richtwerte für die einzelnen Arbeitsschritte bei der initialen Ausgabe von Zertifikaten anzusehen. Die Ausgabe von Folgezertifikaten bzw. Ersatzzertifikaten nach der Sperrung von Zertifikaten können von den angegebenen Werten situationsabhängig abweichen.

4.2.3.1 Ausgabe von initialen Sub-CA Zertifikaten

Die Bearbeitung der Zertifikatsanträge gliedert sich in folgende Arbeitsschritte:

Arbeitsschritt	Beschreibung des Arbeitsschrittes	Zeitrahmen
1	Start des Beantragungsprozesses durch Sub-CA	-
2	Kontaktaufnahme zur Terminvereinbarung durch die Root-CA	1 Kalenderwoche (Die Root-CA soll dabei einen Termin (für Arbeitsschritt 3) innerhalb der nachfolgenden 2 Kalenderwochen ermöglichen)
3	Übergabe der Dokumente / Nachweise im Rahmen eines persönlichen Termins	-

4	Vorprüfung der Unterlagen und Rückmeldung an den Sub-CA Betreiber	1 Kalenderwoche
5 (optional)	Nachlieferungsfrist für den Sub-CA Betreiber	3 Kalenderwochen
6	Prüfung der Unterlagen durch die Root-CA inkl. Rückmeldung an den Sub-CA Betreiber	2 Kalenderwochen
7	Ausstellung der Zertifikate für die Sub-CA	3 Arbeitstage

Tabelle 7 Zeitablauf für die initiale Ausgabe von Sub-CA Zertifikaten

Für die Einhaltung der hier definierten Zeiträume ist eine fristgerechte und fachliche Lieferung / Mitwirkung des Sub-CA Betreibers Voraussetzung. Sollten sich die Lieferungen / Zuarbeiten der Sub-CAs verzögern, können sich die Zeiten verlängern.

Grundsätzlich sind die in Tabelle 7 angegebenen Zeitrahmen als Obergrenze anzusehen.

4.2.3.2 Ausgabe von initialen Endnutzer-Zertifikaten

Die Bearbeitung der Zertifikatsanträge gliedert sich in folgende Arbeitsschritte:

Arbeitsschritt	Beschreibung des Arbeitsschrittes	Zeitrahmen
1	Start des Beantragungsprozesses durch den Endnutzer	-
2	Kontaktaufnahme zur Terminvereinbarung durch die Sub-CA	3 Arbeitstage (Die Sub-CA soll dabei einen Termin (für Arbeitsschritt 3) innerhalb der nachfolgenden 3 Arbeitstage ermöglichen)
3	Übergabe der Dokumente / Nachweise ggf. im Rahmen eines persönlichen Termins	-
4	Vorprüfung der Unterlagen und Rückmeldung an den Endnutzer	1 Kalenderwoche
5 (optional)	Nachlieferungsfrist für den Endnutzer	3 Kalenderwochen
6	Prüfung der Unterlagen durch die Sub-CA inkl. Rückmeldung an den Endnutzer	1 Kalenderwoche
7	Ausstellung der Zertifikate für Endnutzer	2 Arbeitstage

Tabelle 8 Zeitablauf für die initiale Ausgabe von Endnutzer-Zertifikaten

Für die Einhaltung der hier definierten Zeiträume ist eine fristgerechte und fachliche Lieferung / Mitwirkung der Endnutzer Voraussetzung. Sollten sich die Lieferungen /Zuarbeiten der Endnutzer verzögern, können sich die Zeiten verlängern.

Die hier angegeben Werte sind als Richtwerte anzusehen, die von den Sub-CA-Betreibern in der jeweiligen Sub-CA-Policy konkretisiert werden MÜSSEN.

4.2.4 Ausgabe von Zertifikaten

Bei Endnutzer-Zertifikaten SOLLTE, über E-Mail-Transport oder alternativer sicherer Kanäle erfolgen. Die hier angegebenen Zeitwerte sind als Richtwerte anzusehen, die

von den Sub-CA-Betreibern in der jeweiligen Certificate Policy der Sub-CA konkretisiert werden MÜSSEN.

Die initialen Zertifikate MÜSSEN, Folgezertifikate KÖNNEN per E-Mail an den Ansprechpartner gesendet werden. Der Versand per E-Mail KANN unverschlüsselt erfolgen.

4.2.5 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats

Der Ansprechpartner SOLLTE nach der Ausstellung eines initialen Zertifikats per E-Mail informiert werden.

4.3 Annahme von Zertifikaten

Bei den Endnutzer-Zertifikaten MUSS der Ansprechpartner des Zertifikatsnehmers nach Erhalt die Angaben im Zertifikat auf Korrektheit und Vollständigkeit prüfen. Um ein Zertifikat zurückzuweisen, MUSS der Ansprechpartner des Zertifikatsnehmers eine Nachricht an die CA schicken. In einer solchen Nachricht ist der Grund für die Verweigerung der Annahme anzugeben. Bei fehlerhaften Zertifikaten sind, soweit möglich, die fehlerhaften bzw. unvollständigen Einträge zu benennen.

4.3.1 Veröffentlichung von Zertifikaten durch die CA

Alle ausgestellten Zertifikate MÜSSEN direkt nach der Ausstellung in dem Index der jeweiligen CA verankert werden.

4.4 Verwendung von Schlüsselpaar und Zertifikat

4.4.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Zertifikate und die zugehörigen privaten Schlüssel MÜSSEN gemäß ihrem Verwendungszweck eingesetzt werden.

4.4.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Die Verwendung des öffentlichen Schlüssels und des Zertifikats erfolgt gemäß dem vorgesehenen Verwendungszweck.

4.5 Zertifikatserneuerung

Zertifikatserneuerung bedeutet das Ausstellen eines neuen Zertifikats für einen öffentlichen Schlüssel, der bereits zertifiziert wurde. Zertifikatserneuerungen DÜRFEN NICHT erfolgen.

4.6 Zertifizierung nach Schlüsselerneuerung

4.6.1 Wer darf Zertifikate für Schlüsselerneuerungen beantragen?

Jeder PKI-Teilnehmer MUSS darauf achten, rechtzeitig vor Ablauf der Zertifikatslaufzeit ein neues Schlüsselpaar zu generieren und ein Zertifikat zu beantragen.

4.6.2 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Es gibt zwei unterschiedliche Arten der Folgeanträge:

- Folgeanträge über telefonischer Anfrage beim zuständigen Ansprechpartner, oder
- Folgeanträge über eine abgesicherte E-Mail-Kommunikation

Folgeanträge über eine abgesicherte E-Mail-Kommunikation

Bei einem Folgeantrag über die E-Mail-Schnittstelle wird der Zertifikatsrequest vom benannten Ansprechpartner des Zertifikatsnehmers an die jeweilige CA in einer E-Mail gesendet.

Unabhängig von der gewählten Kommunikationsverbindung wird bei einem routinemäßigen Antrag direkt gehandelt und das Zertifikat wird ausgestellt.

4.6.3 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Der Beantragende wird durch die Zustellung des Nachfolgezertifikats informiert.

Die sonstigen Teilnehmer der PKI werden grundsätzlich nicht individuell über die Ausgabe von Zertifikaten zur Schlüsselerneuerung informiert. Eine Benachrichtigung erfolgt nur über die Veröffentlichung im Index der CA.

4.6.4 Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen

Bei den Client-/Server-Zertifikaten MUSS der Ansprechpartner des Zertifikatsnehmers nach Erhalt die Angaben im Zertifikat auf Korrektheit und Vollständigkeit prüfen. Um ein Zertifikat zurückzuweisen, MUSS der Ansprechpartner des Zertifikatsnehmers eine Nachricht an die CA schicken. In einer solchen Nachricht ist der Grund für die Verweigerung der Annahme anzugeben. Bei fehlerhaften Zertifikaten sind, soweit möglich, die fehlerhaften bzw. unvollständigen Einträge zu benennen.

4.6.5 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA

Alle ausgestellten Zertifikate MÜSSEN unmittelbar nach der Ausstellung in dem Index der jeweiligen CA veröffentlicht werden.

4.6.6 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Alle ausgestellten Zertifikate werden direkt nach der Ausstellung in dem Index der jeweiligen CA veröffentlicht.

4.7 Änderungen am Zertifikat

Änderungen an den Zertifikatsinhalten, abgesehen vom Schlüsselmaterial, sind nicht vorgesehen. Sollte sich Änderungsbedarf ergeben, z.B. durch eine Umfirmierung eines Zertifikatsnehmers (d.h. die Änderung des Firmennamens oder der Gesellschaftsform), MUSS ein neues initiales Zertifikat beauftragt und das alte Zertifikat gesperrt werden.

4.8 Sperrung von Zertifikaten

Die Initiierung der Sperrung eines Zertifikats kann durch den Zertifikatsnehmer, die für das Zertifikat zuständige CA und die Root eingeleitet werden.

4.8.1 Sperrung

Alle Zertifikate werden über die von der Root- bzw. Sub-CA bereitgestellten Schnittstellen/Prozesse gesperrt. Eine Sperrung kann nicht zurückgenommen werden.

Alle Sperrungen MÜSSEN unverzüglich umgesetzt und in die neuen Sperrlisten aufgenommen werden.

Ist dem Sperrenden der genaue Zeitpunkt für den Eintritt des Sperrgrundes bekannt, so MUSS dieser bei der Sperrung angegebenen werden, ansonsten erfolgt der Eintrag in die Sperrliste ohne diesen Parameter.

Alle Teilnehmer MÜSSEN immer die aktuelle Sperrliste verwenden. In besonderen Fällen (Erstinbetriebnahme oder auf Aufforderung einer CA-Instanz) MÜSSEN neben den regelmäßigen Aktualisierungen auch neue Sperrlisten abgefragt werden.

4.8.2 Aktualisierungs- und Prüfungszeiten bei Sperrungen

In der folgenden Tabelle sind die minimal erforderlichen Aktualisierungs- und Prüfungszeiten der Sperrlisten für die einzelnen PKI-Teilnehmer definiert. Es wird zwischen regelmäßigen Aktualisierungen, verursacht durch den Ablauf der Gültigkeitszeit einer Sperrliste, und anlassbezogenen Aktualisierungen, verursacht durch die Sperrung von Zertifikaten, unterschieden. Voraussetzung für die anlassbezogene Aktualisierung ist, dass die CA wie in Tabelle 9 definiert erreichbar ist.

Nach Eintreffen eines Antrags für eine Sperrung MUSS dieser von der zugehörigen CA unverzüglich geprüft werden. Ist der Antrag valide MUSS dieser zeitlich, wie in Tabelle 9 definiert, umgesetzt werden.

Die Gültigkeit einer Sperrliste darf max. 3 Tage länger sein, als das in Tabelle 9 definierte Aktualisierungsintervall.

Sollte eine Sperrliste nicht verfügbar bzw. abrufbar sein, MUSS ersatzweise mit der zuletzt bekannten Sperr- liste weitergeprüft werden. Die für die Sperrliste verantwortliche CA MUSS hierüber unverzüglich informiert werden (über Kontaktadresse in der CP der jeweiligen CA). Diese MUSS dann auf anderem Wege eine aktuelle Sperrliste zur Verfügung stellen. Den Zertifikaten der entsprechenden CA kann in diesem Fall nicht vertraut werden.

PKI-Teilnehmer		Regelmäßige Aktualisierung der Sperrliste	Erreichbarkeit für Sperrungen	Anlassbezogene Aktualisierung der Sperrliste	Abruf der Sperrliste	Prüfung der Zertifikate auf Sperrung
Root-CA	Root-CA-CRL	Innerhalb von 30 Tagen	Täglich	Unverzüglich	Entfällt (Keine übergeordnete Sperrliste)	Entfällt (Keine übergeordnete Sperrliste)
	Root-TLS-CRL	Innerhalb von 7 Tagen				
Sub-CA		Innerhalb von 7 Tagen	Täglich	Unverzüglich	Täglich	Täglich
Endnutzer		Entfällt (Erstellt keine Sperrliste)	Entfällt	Entfällt (Erstellt keine Sperrliste)	Täglich	Bei jeder Verwendung

Tabelle 9 Zeitliche Anforderungen bei Sperrungen

4.9 Service zur Statusabfrage von Zertifikaten

Für die PKI ist kein OCSP-Dienst vorgesehen. Statusabfragen hinsichtlich einer Sperrung können über die entsprechende CRL erfolgen.

4.10 Beendigung der Teilnahme

Die Beendigung der Teilnahme eines Zertifikatsnehmers kann durch diesen selbst oder die zugehörige CA eingeleitet werden.

Die Beendigung gliedert sich in drei Schritte:

- Information der Zertifikatsnutzer, die direkt von einer Beendigung der Teilnahme des Zertifikatsinhabers betroffen sind, durch den Zertifikatsinhaber. Es muss hierbei durch den Zertifikatsinhaber jedes Unternehmen informiert werden, welches im Rahmen der Nutzung der Zertifikate mit dem Zertifikatsinhaber in Kontakt stand.
- Austausch der von der Sperrung betroffenen Zertifikate, so dass ein kontinuierlicher Betrieb gewährleistet werden kann (hierzu MUSS eine entsprechende Abstimmung zwischen den Beteiligten bezüglich des dazu notwendigen Zeitrahmens erfolgen. Ausgenommen hiervon ist die Sperrung von Zertifikaten aufgrund von Gefahren für den sicheren Betrieb der PKI).
- Sperrung aller Zertifikate des Zertifikatsnehmers sowie entsprechende Kennzeichnung der bekannten Zertifikate der benannten Ansprechpartner

zum betroffenen Zertifikatsnehmer, so dass die Nutzung der Zertifikate für eine vertrauliche und authentische Kommunikation unterbunden wird.

4.11 Hinterlegung und Wiederherstellung von Schlüsseln

Für die Root-CA MUSS eine Hinterlegung für die Schlüssel und Zertifikate durchgeführt werden.

Sub-CAs und andere PKI Teilnehmer KÖNNEN eine Hinterlegung (z.B. für die Katastrophenfallvorsorge) gemäß den definierten Sicherheitsanforderungen durchführen. Der entsprechende Hinterlegungsprozess muss nachvollziehbar dokumentiert werden.

5 Organisatorische, betriebliche und physikalische Sicherheitsanforderungen

Die PKI Policy spezifiziert technische und organisatorische Sicherheitsanforderungen an alle PKI-Teilnehmer, die im Kontext der PKI relevant sind, um die Sicherheit der PKI zu gewährleisten.

5.1 Generelle Sicherheitsanforderungen

In diesem Abschnitt werden die generellen Sicherheitsanforderungen an die PKI-Teilnehmer definiert. Diese bilden den Sicherheitsrahmen für die PKI-Teilnehmer. Hierauf aufbauend werden in dieser PKI Policy erweiterte Sicherheitsanforderungen definiert.

Die Gewährleistung geeigneter infrastruktureller, organisatorischer und personeller Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb einer PKI. Die für den konkreten Betrieb der PKI relevanten Sicherheitsmaßnahmen sind im technischen Konzept zur Installation und zum Betrieb der PKI des Abrechnungszentrums Emmendingen beschrieben und ist Teil der internen betrieblichen Dokumentation.

Allgemeine Sicherheitsanforderungen an das Abrechnungszentrum Emmendingen als Betreiber der Root-CA und Sub-CA sind in der Sicherheitsleitlinie sowie verschiedenen Sicherheitsrichtlinien des Abrechnungszentrums Emmendingen festgelegt.

5.2 Erweiterte Sicherheitsanforderungen

5.2.1 Betriebsumgebung und Betriebsabläufe

Nachfolgend werden die Anforderungen an eine sichere Betriebsumgebung und an sichere Betriebsabläufe für die Root-CA, Sub-CAs definiert.

- **Objektschutz:** Die betrieblichen Prozesse MÜSSEN vor Störung geschützt werden.
- **Zutrittssicherheit:** Es MÜSSEN Vorkehrungen zur Sicherung des Zutritts vor Unbefugten zu den jeweiligen Betriebsräumen getroffen werden.
- **Geschäftsfortführung:** Die Wiederaufnahme der Betriebsabläufe sowie die Wiederherstellung der notwendigen Ressourcen (Personal, Technologie, Standort, Information) MÜSSEN nach einer Unterbrechung unverzüglich erfolgen.
- **Informationsträger:** Bei der Verarbeitung und Aufbewahrung von Informationen in IT-Systemen MUSS der Schutz vor unautorisiertem oder unbeabsichtigtem Gebrauch gewährleistet werden. Wenn nicht mehr benötigt, MUSS der Informationsträger sicher und unwiederherstellbar zerstört werden.
- **Brandschutz:** Es MÜSSEN bei den CAs Maßnahmen getroffen werden, die der Entstehung eines Brandes und der Ausbreitung von Feuer vorbeugen sowie wirksame Löscharbeiten ermöglichen.

- **Strom:** Eine gesicherte Stromversorgung einschließlich Redundanzkonzept für Strom SOLLTE bei den CAs gewährleistet werden.
- **Wasserschaden:** Die IT-Infrastruktur SOLLTE bei CAs gegen das Eintreten eines Wasserschadens geschützt werden.
- **Notfall-Management und Wiederherstellung:** Die CAs MÜSSEN ihre Systeme durch Backup-Mechanismen sichern, um die Wiederherstellung des Betriebs nach einer Störung oder einem Notfall zu ermöglichen. Nur vertrauenswürdiges Betriebspersonal SOLLTE Backup- und Wiederherstellungsprozesse durchführen.

5.2.2 Verfahrensanweisungen

Für den Betrieb der Root-CA und einer Sub-CA MÜSSEN folgende Verfahrensanweisungen umgesetzt werden:

- **Einhaltung von Verpflichtungen:** Basierend auf den verschiedenen Aufgaben MÜSSEN die Mitarbeiter die Pflichten entsprechend ihren Rollen bei ihren Tätigkeiten einhalten.
- **Vertreterreglung:** Für jede definierte Rolle MUSS ein Vertreter ernannt werden.
- **Verantwortungsbereiche:** Die Verantwortungsbereiche der Mitarbeiter MÜSSEN klar definiert werden. Für die Verantwortungsbereiche MÜSSEN klare Rollen definiert werden.
- **Vier-Augen-Prinzip:** Kritische Vorgänge erfordern die Einhaltung des Vier-Augen-Prinzips. Nach Möglichkeit soll das Vier-Augen-Prinzip auch technisch durchgesetzt werden. Es ist immer zu dokumentieren, welche beiden Personen einen kritischen Vorgang durchgeführt haben.
- **Beschränkung der Anzahl Mitarbeiter:** Die Anzahl der Personen, die sicherheitsrelevante oder kritische Funktionen durchführen, MUSS auf die unbedingt notwendige Anzahl begrenzt sein.
- **Eskalationsmanagement:** Es MUSS ein gut definiertes und eindeutiges Eskalationsmanagement umgesetzt werden.

Ein EZT MUSS folgende der oben aufgeführten Verfahrensanweisungen umsetzen:

- **Einhaltung von Verpflichtungen**
- **Beschränkung der Anzahl Mitarbeiter**

5.2.3 Personal

Der Betrieb der Root-CA und der Sub-CAs MUSS durch angemessen geschultes und erfahrenes Personal erfolgen. Insbesondere sollen folgende Anforderungen umgesetzt werden:

- **Rollen und Verantwortungen:** Die Rollen und Verantwortlichkeiten sind zu dokumentieren. In Bezug auf kritische Aufgaben/Funktionen bezüglich des Schlüssel- und Zertifikatsmanagement-Lebenszyklus MÜSSEN die

Verantwortlichkeiten klar definiert werden.
Jede Instanz in einer Organisation MUSS je nach zugrundeliegender PKI-Rolle (siehe Tabelle 2 Übersicht der PKI-Teilnehmer) über ein Rollen- und Rechtekonzept verfügen. Dies ist Gegenstand der betrieblichen Dokumentation. Hierbei MUSS technisch und oder organisatorisch sichergestellt werden, dass die Trennung der Instanzen hinsichtlich der Durchführung der PKI relevanten Prozesse, insbesondere die Beantragung und Ausstellung von Zertifikaten, nicht umgangen werden kann.

- **Rollenbeschreibungen:** Für temporäres und permanentes Personal MÜSSEN Rollenbeschreibungen definiert werden, welche Aufgabentrennung, Mindestberechtigungen, Sicherheitsprüfungen, Verpflichtung zu Mitarbeiter- und Sensibilisierungsschulungen enthalten.
- **Einhaltung der ISMS-Anforderungen:** Das Personal MUSS administrative und betriebliche Verfahren und Prozesse im Einklang mit der Sicherheitsleitlinie und den Sicherheitsrichtlinien des Abrechnungszentrums Emmendingen.
- **Qualifiziertes Personal:** Die CA MUSS Personal beschäftigen, welches über die erforderlichen Fachkenntnisse, Erfahrung und Qualifikation für das Aufgabenfeld und die angebotenen Dienste verfügt.
- **Sicherheitsüberprüfung:** Die CA MUSS sicherstellen, dass an kritischen und sicherheitsrelevanten Prozessen beteiligte Personen bezüglich der persönlichen Eignung geprüft und die Prüfung dokumentiert wurde.

5.2.4 Monitoring

Folgende Ereignisse MÜSSEN erkannt und aufgezeichnet bzw. dokumentiert werden:

Root-CA und Sub-CA:

- Schlüsselmanagement
- Nutzung des privaten Schlüssels der CA, insbesondere zur Erstellung von Zertifikaten
- Nicht routinemäßige Ausstellung von Zertifikaten
- Es MUSS sichergestellt werden, dass unautorisierter oder unbeabsichtigter Gebrauch von PKI-relevanten Systemen erkannt wird.

EZT:

- Schlüsselmanagement

5.2.5 Archivierung von Aufzeichnungen

Es MUSS sichergestellt sein, dass die Systeme über angemessene Archivierungsfunktionen verfügen. Die Zeiträume sind in Anhang B dokumentiert. Folgende Anforderungen MÜSSEN berücksichtigt werden:

Root-CA und Sub-CA:

- **Archivierung der öffentlichen Schlüssel:** Die Beteiligten MÜSSEN sicherstellen, dass die relevanten Informationen zu den öffentlichen Schlüsseln des Zertifikates archiviert werden.
- **Eindeutige Zuordnung von Zertifikaten:** Die Beteiligten MÜSSEN in der Lage sein, die jeweiligen Zertifikate eindeutig den registrierten Benutzern zuzuordnen.
- **Verfügbarkeit:** Mit Hilfe einer angemessenen Archivierung klar definierter Daten der verbreiteten öffentlichen Zertifikatsschlüssel MUSS nach einer vollständigen Wiederherstellung die Verfügbarkeit der Dienste gewährleistet werden.
- **Datenbanken:** Die Aktualität, Integrität und Vertraulichkeit der Datenbanken MÜSSEN gewährleistet sein, insbesondere bezüglich der Konsistenz der Datenbanken zur Verbreitung von Zertifikaten und der Datenbank zur Nutzer-Registrierung.
- **Definition der zu archivierenden Informationen:** Die Informationen, welche für das Tracking und die Wiederherstellung von öffentlichen Schlüsseln benötigt werden, MÜSSEN klar definiert werden.
- **Die zu archivierenden Informationen für öffentliche Schlüssel MÜSSEN enthalten:**
    - Registrierungsinformationen
    - Essentielle CA-Ereignisse (z.B. Generierung von Zertifikaten)
    - Schlüsselverwaltung
    - Zertifizierungsereignisse
    - Für jedes Ereignis MUSS der Zeitpunkt der Archivierung präzise festgelegt werden.
- **Zu archivierende Ereignisse:** Die wesentlichen Ereignisse, die archiviert werden, umfassen:
    - Zertifikatserstellung
    - Erneuerung und Aktualisierung der öffentlichen Zertifikats-Schlüssel
    - Incident- oder Notfall-Management bezüglich Zertifikats-relevanter Vorfälle.
- **Verlorene Schlüssel / Zertifikate:** Daten von verbreiteten Schlüsseln / Zertifikaten DÜRFEN NICHT wiederhergestellt werden. Es MÜSSEN neue Schlüssel / Zertifikate beantragt werden.

EZT MUSS folgende der oben aufgeführten Verfahrensanweisungen umsetzen:

- **Archivierung der öffentlichen Schlüssel**
- **Zu archivierende Ereignisse**
    - Zertifikatsbeantragung
    - Incident- oder Notfall-Management bezüglich Zertifikatsrelevanter Vorfälle.

5.2.6 Schlüsselwechsel einer Zertifizierungsstelle

Der Schlüsselwechsel einer Zertifizierungsstelle kann einerseits geplant und andererseits ungeplant erfolgen:

- **Geplanter Schlüsselwechsel:** Im Fall eines planbaren Schlüsselwechsels einer Zertifizierungsstelle MÜSSEN die in beschriebenen Verfahren berücksichtigt werden und entsprechende Prozesse vorhanden sein.
- **Ungeplanter Schlüsselwechsel:** Für den Fall, dass ein unvorhergesehener Schlüsselwechsel einer Zertifizierungsstelle notwendig ist, MÜSSEN entsprechende Verfahren im Notfallmanagement definiert werden.
- Sowohl ein geplanter als auch ein ungeplanter Schlüsselwechsel einer Zertifizierungsstelle MUSS gemäß dem **Vier-Augen-Prinzip** erfolgen.

5.2.7 Auflösen einer Zertifizierungsstelle

Root-CA: Die Root-CA kann nicht aufgelöst werden. Dies würde die Einstellung des gesamten Betriebs der PKI bedeuten.

Sub-CA: Wenn eine Sub-CA aufgelöst wird, MÜSSEN alle von ihr ausgestellten Zertifikate gesperrt werden. Insbesondere gelten folgende Anforderungen:

- Übertragung der Aufgaben und Verpflichtungen: Im Falle der Auflösung einer Sub-CA MÜSSEN deren Aufgaben und Verpflichtungen für eine Übergangszeit aufrechterhalten oder bei einer endgültigen Auflösung von einer Nachfolgeorganisation übernommen werden. Dies umfasst die Bereitstellung von Sperrinformationen für die Restlaufzeit der ausgegebenen Zertifikate.
- Informationspflicht: Eine Sub-CA MUSS im Falle ihrer Auflösung alle beteiligten Teilnehmer sowie weitere Organisationen, mit denen Vereinbarungen bestehen, vor der Kündigung der Dienstleistung rechtzeitig informieren.
- Zerstörung von Schlüssel- und Zertifikatsinformationen: Nach Einstellung der Tätigkeiten MÜSSEN alle privaten Schlüssel einschließlich Zertifikatsinformationen und zugehörige Kundendaten zerstört werden.

5.2.8 Aufbewahrung der privaten Schlüssel

Alle Teilnehmer der PKI KÖNNEN folgende Anforderung umsetzen:

- **Kryptografiemodule:** Die Schlüssel KÖNNEN in vertrauenswürdigen Kryptografiemodulen gespeichert werden. Wenn private Schlüssel der Root-CA, Sub-CA und ggf. von Teilnehmern außerhalb des Sicherheitsmoduls (z.B. als Backup) aufbewahrt werden, MÜSSEN diese mit dem gleichen Schutzniveau, wie bei der Schlüsselerstellung verarbeitet werden.

Die Root-CA, Sub-CA MÜSSEN sicherstellen, dass folgende Anforderungen umgesetzt werden:

- **Schutz der Speichermedien:** Die Speichermedien MÜSSEN gegen nicht autorisierte Nutzung, Schäden durch Personen und weitere Bedrohungen (z.B. Feuer) gesichert werden.

- **Schlüsselaufbewahrung:** Die Speichermedien MÜSSEN sich in einem physisch und logisch gesicherten Bereich befinden. Der Zutritt MUSS auf eine klar definierte Anzahl von Personen eingeschränkt werden.
- **Vertrauenswürdiges Personal:** Der private Schlüssel DARF NUR durch vertrauenswürdiges Personal erzeugt, gespeichert und für Signaturen verwendet werden.
- **Abfallbeseitigung:** Es MUSS sichergestellt werden, dass Abfälle nicht unberechtigt genutzt und vertrauliche Informationen veröffentlicht werden können.
- **Gehärtete IT-Systeme:** Es MUSS sichergestellt werden, dass die Anforderungen an gehärtete IT-Systeme und Netzwerke sowie an die physische Sicherheit eingehalten werden.

Ein EZT MUSS folgende der oben genannten Anforderungen umsetzten:

- **Schüsselaufbewahrung**
- **Vertrauenswürdiges Personal**
- **Abfallbeseitigung**

5.2.9 Behandlung von Vorfällen und Kompromittierung

Nachfolgend wird beschrieben, wie bei Vorfällen und Kompromittierungen verfahren werden MUSS:

- Bei einer Kompromittierung oder einem begründeten Verdacht auf Kompromittierung eines privaten Schlüssels MUSS das zugehörige Zertifikat unverzüglich gesperrt und DARF NICHT wiederverwendet werden.
- Ein Fall von Kompromittierung sowie Verdachtsfälle MÜSSEN durch den Schlüsselinhaber dokumentiert werden.
- Jeder Verdacht auf Kompromittierung oder Missbrauch des privaten Schlüssels ist aufzuklären.
- Die Generierung neuer Schlüssel und Zertifikate MUSS überwacht und dokumentiert werden.

5.2.10 Meldepflichten

Bei Kompromittierung oder anderweitigen sicherheitsrelevanten Vorfällen MUSS eine Meldung aufbereitet und an die zuständige CA kommuniziert werden. Die Meldepflicht liegt auf Seiten des Zertifikatsnehmers. Bei der Kompromittierung einer Sub-CA MUSS zusätzlich die Root informiert werden.

Folgende Vorkommnisse sind Beispiele für eine Meldepflicht:

- Kompromittierung des privaten Schlüsselmaterials
- Verstoß gegen relevante Betriebsauflagen
- Betreiber der CA ist nicht mehr aktiv (Bsp.: Insolvenz)

- Aufforderung zur Sperrung oder Suspendierung eines Zertifikates

Folgende Angaben MÜSSEN der Meldung mindestens beigefügt werden:

- Was wurde kompromittiert bzw. was wurde betroffen?
- Wann ist das Vorkommnis passiert bzw. wann wurde der Vorfall bemerkt?
- Wer hat das Vorkommnis festgestellt?
- Ort des Vorkommnisses
- Wie ist das Vorkommnis vermutlich abgelaufen?
- Wenn schon eine Maßnahme durchgeführt wurde: Welche Maßnahmen wurden schon eingeleitet?

Root:

Folgende Meldepflichten auf Seiten der Root erfolgen via Veröffentlichung über die PKI-Webseite (siehe Tabelle 6):

- Änderungen dieser PKI Policy,

Jede Meldung MUSS nachvollziehbar dokumentiert werden und so abgelegt werden, dass die Meldung im Bedarfsfall vorgezeigt werden kann. Der Verfasser der Meldung MUSS eindeutig gekennzeichnet sein.

5.2.11 Notfall-Management

Die Root-CA, Sub-CA und EZT MÜSSEN gewährleisten, dass die Wiederherstellung des Normalbetriebs nach einer Störung oder nach einem Notfall innerhalb einer angemessenen Frist erfolgt. Notfall-Szenarien betreffen u.a.:

- Kompromittierung des privaten Schlüssels
- Entdeckte Schwachstellen in den verwendeten kryptografischen Verfahren
- Nichtverfügbarkeit von Sperrlisten

Insbesondere gelten folgende Anforderungen, welche erfüllt werden MÜSSEN:

- **Notfallmanagement:** Die Root-CA, Sub-CA und EZT MÜSSEN rechtzeitig angemessen auf Störungen oder Notfälle reagieren, um Schäden zu minimieren und den Geschäftsbetrieb zu gewährleisten.
- **Maßnahmenplanung:** Die Root-CA MUSS angemessene Maßnahmen für den Fall vorbereiten, dass relevante Algorithmen gebrochen oder Verfahren unsicher werden.
- **Kompromittierung:** Wenn die Vermutung besteht, dass Schlüsselmaterial kompromittiert ist, so DARF KEIN PKI-Teilnehmer dieses weiter nutzen.
- **Risikoreduktion / Schadensminderung:** Alle PKI-Teilnehmer SOLLTEN entsprechende Maßnahmen zur Minimierung von Risiken und Schäden anwenden.
- **Vermeidung von Vorfällen:** Alle PKI-Teilnehmer MÜSSEN angemessene Maßnahmen vorbereiten sowie die Ursachen von Vorfällen ermitteln, um diese in Zukunft zu vermeiden.

- **Notfallpläne:** Die Root-CA und Sub-CA MÜSSEN entsprechende Pläne vorbereiten, um die Geschäftsprozesse nach einem Notfall wiederherzustellen.
- **Backups:** Die Root-CA und Sub-CA MÜSSEN Backups von privaten und öffentlichen Schlüsseln, ausgestellten Zertifikaten und Sperrinformationen durchführen.
- **Vorgehen nach einer Störung:** Nach einer schweren Störung MÜSSEN alle PKI-Teilnehmer sicherstellen, dass die entstandene Sicherheitslücke geschlossen wird.

6 Technische Sicherheitsanforderungen

6.1 Erzeugung und Installation von Schlüsselpaaren

Jeder Zertifikatsnehmer MUSS sein eigenes Schlüsselpaar generieren.

6.1.1 Generierung von Schlüsselpaaren für die Zertifikate

Die PKI-Teilnehmer Root-CA und Sub-CA MÜSSEN sicherstellen, dass folgende Anforderungen umgesetzt werden:

- **Generierung im Vier-Augen-Prinzip:** Das Schlüsselpaar MUSS während der Schlüsselzeremonie im Vier-Augen-Prinzip unter Teilnahme des für den Schlüssel verantwortlichen Mitarbeiters generiert werden.
- Der **technische Zugriff auf die Schlüssel in den Kryptografiemodulen** aller Zertifikatsnehmer MUSS durch ein Geheimnis geschützt werden (Passwort, PIN, o.ä.), welches ausschließlich die jeweiligen Operatoren kennen. Der Zugriff auf das Kryptografiemodul, insbesondere zur Schlüsselerzeugung, MUSS auf ein Minimum an Operatoren beschränkt sein.

6.1.2 Lieferung privater Schlüssel

Die Erstellung der privaten Schlüssel erfolgt dezentral durch die Zertifikatsnehmer der PKI. Alternativ MÜSSEN die privaten Schlüssel bei Bereitstellung durch die Root CA oder Sub CA über einen Kryptografie-gesicherten Transport übertragen werden.

6.1.3 Lieferung öffentlicher Zertifikate

Alle Zertifikate werden in den jeweiligen Verzeichnissen der ausstellenden CAs abgelegt und sind somit für alle PKI-Teilnehmer zugänglich.

6.1.4 Schlüssellängen und kryptografische Algorithmen

Schlüssellängen und kryptografische Algorithmen der Schlüsselpaare MÜSSEN angemessene kryptografische Verfahren einhalten.

Bei der Erzeugung und Nutzung von statischen und temporären Schlüsseln im Rahmen der PKI MUSS ein Zufallsgenerator verwendet werden. Des Weiteren SOLLTE bei statischen Schlüsseln ein Kryptografiemodul eingesetzt werden.

6.1.5 Festlegung der Parameter der Schlüssel und Qualitätskontrolle

- **Sichere Handhabung und Lagerung von Schlüsselmaterial:** Software- und Hardware-Komponenten zur Erzeugung, Handhabung und Lagerung der privaten Schlüssel MÜSSEN angemessene Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial einhalten.
- **Defektes Krypto-Modul (KM):** Im Falle eines defekten KM ist sicherzustellen, dass das Schlüssel-Backup sicher und im Vier-Augen-Prinzip in ein neues KM nach angemessenen Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial importiert wird.

- **Schutz vor Angriff auf den privaten Schlüssel:** Es MUSS sichergestellt werden, dass der private Schlüssel nicht von einem Angreifer für kryptografische Operationen missbraucht werden kann und dass angemessene Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial und gehärteten IT-Systemen und Netzwerken eingehalten werden.
- **Unverschlüsselter / unberechtigter Export des privaten Schlüssels:** Es MUSS sichergestellt werden, dass der private Schlüssel nicht unverschlüsselt oder unberechtigt aus dem Schlüsselspeicher exportiert werden kann. Es MÜSSEN angemessene Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial eingehalten werden.

6.1.6 Verwendungszweck der Schlüssel

Die Schlüssel DÜRFEN ausschließlich für die beschriebenen Verwendungszwecke eingesetzt werden. Der Verwendungszweck ist in der jeweils aktuellen Fassung der CP konkretisiert.

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptografische Module

Die Teilnehmer der PKI KÖNNEN Kryptografiemodule zur Generierung, Speicherung und Nutzung ihrer privaten Schlüssel zu ihren Zertifikaten aus der PKI verwenden.

Neben dem Einsatz eines sicheren Kryptografiemodules MUSS auch ein sicherer Umgang mit den privaten Schlüsseln sichergestellt werden.

6.2.1 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln

Das Schlüsselmanagement bei Root-CA, Sub-CA MUSS im Vier-Augen-Prinzip, unter entsprechender Dokumentation und Protokollierung insbesondere der Rollen und eindeutiger Identifikation der teilnehmenden Personen, durchgeführt werden.

6.2.2 Ablage privater Schlüssel

Es MUSS sichergestellt werden, dass die Daten der privaten Schlüssel zur sicheren Handhabung und Lagerung von Schlüsselmaterial gespeichert werden.

6.2.3 Backup privater Schlüssel

Die Root-CA und Sub-CA MÜSSEN sicherstellen, dass Maßnahmen zum sicheren Backup der privaten Schlüssel umgesetzt werden. Insbesondere MÜSSEN folgende Anforderungen eingehalten werden:

- Die Vorgaben zum **Transfer** privater Schlüssel in oder aus kryptografischen Modulen MÜSSEN eingehalten werden.
- **Sichere Schlüssel-Backups:** Die Durchführung von sicheren Backups der privaten Schlüssel MUSS nach den Vorgaben zur sicheren Handhabung und Lagerung von Schlüsselmaterial durchgeführt werden.

- **Durchführung des Schlüssel-Backups:** Das Schlüssel-Backup MUSS während der Schlüsselzeremonie gemäß dem Vier-Augen-Prinzip unter Teilnahme des für den Schlüssel verantwortlichen Mitarbeiters durchgeführt werden. Automatisierte Prozesse zur Übertragung der Schlüssel auf ein weiteres HSM (z.B. für ein Cold-Standby-Backup) DÜRFEN genutzt werden.
- Schlüsselspeicherung: Es MUSS sichergestellt werden, dass die Backup-Daten des öffentlichen Schlüssels nach den Vorgaben zur sicheren Handhabung und Lagerung von Schlüsselmaterial gespeichert werden.
- Zugriff auf Backup-Daten: Es MUSS sichergestellt werden, dass nur vertrauenswürdige Mitarbeiter Zugriff auf die Schlüsselspeicher- und Backup-Daten haben.

Es wird EMPFOHLEN, dass der EZT ein Backup durchführt. Sobald ein Backup durchgeführt wird, SOLLTEN die vorstehenden Anforderungen eingehalten werden.

Der private Schlüssel KANN als Backup wie folgt exportiert werden:

- Verschlüsselter Dateicontainer:
    - Datenstruktur, die den geheimen Schlüssel enthält und mit einem KEK (Key Encryption Key) verschlüsselt ist.
    - Die Nutzung des Dateicontainers erfordert den Import in ein Kryptografiemodul.
    - Der Zugriff auf den verschlüsselten Dateicontainer MUSS auf das Betriebspersonal beschränkt sein.
    - Die Wiederherstellung des Dateicontainers ist technisch ausschließlich im 4-Augen-Prinzip möglich.
- Backup Kryptografiemodul:
    - Der private Schlüssel wird verschlüsselt direkt in das Backup-Kryptografiemodul importiert.
    - Der Zugang zum Backup-Kryprografiemodul MUSS auf das Betriebspersonal beschränkt sein.

6.2.4 Archivierung privater Schlüssel

Es wird keine Archivierung gesperrter oder abgelaufener privater Schlüssel durchgeführt.

6.2.5 Transfer privater Schlüssel in oder aus kryptografischen Modulen

- Der private Schlüssel KANN zwischen kryptografischen Modulen transferiert werden.
- Voraussetzung für den Transfer privater Schlüssel ist, dass nur Kryptografiemodule verwendet werden, welche die Anforderungen erfüllen.
- Der private Schlüssel MUSS hierbei verschlüsselt und integritätsgesichert transferiert werden. Die Ver-/ & Entschlüsselung MUSS in den Kryptografiemodulen erfolgen.
- Der KEK zur Ver-/Entschlüsselung des privaten Schlüssels MUSS vertraulich und integritätsgesichert ausgetauscht werden.

- Bei der Durchführung eines manuellen Transfers MUSS das Vier-Augen-Prinzip eingehalten werden.

6.2.6 Speicherung privater Schlüssel in kryptografischen Modulen

- Grundsätzlich KÖNNEN die privaten Schlüssel eines PKI-Teilnehmers auf einem Kryptografiemodul gespeichert werden.
  Die einzige Ausnahme bilden die client- und serverseitigen TLS-Schlüssel bei Sub-CA und Root-CA, die bei der Root-CA und den Sub-CAs zur TLS-Authentisierung verwendet werden.
- Auf einem HSM DÜRFEN private Schlüssel von PKI-Teilnehmern derselben PKI-Rolle gespeichert werden (Bsp.: es dürfen mehrere CA-Schlüssel auf demselben HSM gespeichert werden). Diese MÜSSEN aber in getrennten Sicherheitsdomänen (Trennung auf Anwendungsebene) verwaltet werden. Entsprechend MÜSSEN diese im HSM logisch getrennt sein.
- Auf einem HSM DÜRFEN KEINE privaten Schlüssel von verschiedenen PKI-Rollen gespeichert werden. Es darf entsprechend keine Vermischung von Schlüsseln von unterschiedlichen PKI-Rollen auf einem HSM erfolgen (Bsp.: es dürfen keine CA- und Client/Server-Schlüssel auf demselben HSM gespeichert werden).

6.2.7 Aktivierung privater Schlüssel

Die Aktivierung eines Schlüssels in einem Kryptografiemodul erfordert die Einhaltung des Vier-Augen-Prinzips.

6.2.8 Deaktivierung privater Schlüssel

Im deaktivierten Zustand der Schlüssel DÜRFEN diese NICHT genutzt werden können.

6.2.9 Zerstörung privater Schlüssel

Die privaten Schlüssel eines CA-Betreibers MÜSSEN in folgenden Fällen sicher und unwiederherstellbar zerstört werden:

- Der Gültigkeitszeitraum des CA-Schlüssels ist abgelaufen
- Der Schlüssel der CA wurde gesperrt.

Die Backups der Schlüssel MÜSSEN ebenfalls berücksichtigt werden.

Die Zerstörung der privaten Schlüssel MUSS durch einen sicheren Lösch-Mechanismus im Kryptografiemodul (falls vorhanden) oder durch die unwiederherstellbare mechanische Zerstörung erfolgen.

Die ENC-Schlüssel sind von dieser Anforderung ausgenommen. Diese dürfen nur noch für die Entschlüsselung abgelegter Daten genutzt werden, mit dem Ziel einer

Umschlüsselung auf den aktuellen ENC-Schlüssel. Sollte der ENC-Schlüssel nicht mehr zur Umschlüsselung erforderlich sein, MUSS dieser ebenfalls zerstört werden.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Die Zertifikate eines Teilnehmers der PKI MÜSSEN inklusive der Statusdaten archiviert werden.

6.3.2 Gültigkeitszeitraum von Zertifikaten und Schlüsselpaaren

Der Gültigkeitszeitraum von Zertifikaten und Schlüsseln ist im technischen Konzept zur Installation und Betrieb definiert.

Unabhängig vom Gültigkeitszeitraum MÜSSEN die folgenden Zertifikate spätestens in dem hierzu angegebenen Intervall gewechselt werden.

Instanz	Zertifikat	Intervall
Root-CA	C(Root)	Alle 5.25 Jahre
	C_{CRL-S}(Root)	Alle 5.25 Jahre
	C_{TLS-S}(Root)	Alle 5.25 Jahre
Sub-CA	C(Sub-CA)	Alle 5 Jahre

Tabelle 10 Intervall Zertifikatswechsel bei einer CA

Sobald eine CA über ein neues Zertifikat verfügt, MUSS dieses zum Ausstellen neuer Zertifikate und der zugehörigen Sperrlisten verwendet werden.

6.4 Aktivierungsdaten

Die Aktivierungsdaten für die Kryptografiemodule MÜSSEN sicher aufbewahrt werden.

6.5 Sicherheitsanforderungen für die Rechneranlagen

Nachfolgend wird die Anforderung an die Rechneranlagen definiert, die von den jeweiligen PKI-Teilnehmern umgesetzt werden MÜSSEN:

- **Root-CA, Sub-CA: Netzwerkkontrolle:** Es MÜSSEN entsprechende Maßnahmen umgesetzt werden, um das interne Netzwerk vom externen zu trennen und vor unbefugtem Zugriff zu schützen.
- **Root-CA, Sub-CA: Intrusion Detection Systeme (IDS):** Der Einsatz von Intrusion-Detection-Systemen (IDS) im gesicherten Netzsegment MUSS berücksichtigt werden. Die Log-Dateien des IDS MÜSSEN regelmäßig kontrolliert werden.
- **Root-CA, Sub-CA: System-Härtung:** Die CA-Server, die zur Erstellung von Zertifikaten verwendet werden, MÜSSEN gehärtet werden. Dies umfasst die Konfiguration und Einstellung der verwendeten Hardware- und Software-Komponenten.

- **Root-CA, Sub-CA: System-Konfiguration:** Die Konfigurationsoptionen und -einstellungen DÜRFEN nur die minimal benötigten Funktionalitäten für den CA Betrieb enthalten.
- **Root-CA, Sub-CA: Netzwerk-Separierung:** Die Netzwerke, in denen sich die CA-Server befinden, MÜSSEN durch geeignete Maßnahmen geschützt werden.
- **Alle PKI-Teilnehmer: Software-Updates:** Software-Updates MÜSSEN bei sicherheitsrelevanten Änderungen schnellstmöglich eingespielt werden, andere Updates SOLLTEN regelmäßig aktualisiert werden.
- **Root-CA, Sub-CA: Vertraulichkeit und Integrität:** Die CA MUSS sensitive Daten vor unbefugtem Zugriff oder Veränderung schützen.
- **Root-CA, Sub-CA: Logging und Audit-Trails:** Log-Dateien und Audit-Trails MÜSSEN regelmäßig geprüft werden, und automatisierte Benachrichtigungen MÜSSEN auf Abweichung vom vorgesehenen Betrieb hinweisen.
- **Root-CA, Sub-CA: Speicherort von Log-Dateien:** Die Dateien der Audit-Trails SOLLEN NICHT auf dem CA-Server, der für die Verwaltung von Zertifikaten verwendet wird, gespeichert werden. Der Speicherort für Log-Dateien KANN temporär der CA-Server sein. Die Log-Dateien MÜSSEN dann regelmäßig auf einen anderen Speicherort ausgelagert werden.
- **Alle PKI-Teilnehmer:** Das System MUSS über eine angemessene Benutzerverwaltung verfügen.
- **Root-CA, Sub-CA: Systemfunktionen:** Die CA MUSS den Zugriff auf die benötigten Systemfunktionen und Hilfsprogramme begrenzen.
- **Alle PKI-Teilnehmer: Schutz vor Schadsoftware:** Die Integrität der System-Komponenten und Informationen MUSS gegen Viren, Schadsoftware sowie nicht zugelassene Programme geschützt werden.

6.6 Zeitstempel

Keine Anforderungen an Zeitstempel.

7 Profile für Zertifikate und Sperrlisten

7.1 Profile für Zertifikate und Zertifikatsrequests

Das Namensschema zu den Zertifikaten ist in Anhang A dieser PKI Policy definiert.

Die Struktur der Sperrlisten, das Sperrmanagement (Veröffentlichung, Aktualisierung und Sperrlistenvalidierung) wird in der jeweils aktuellen Fassung der CP definiert.

7.2 Zugriffsrechte

Die erlaubte Funktion der Zertifikate wird über die Key-Usage-Extension definiert.

7.3 Zertifikatserweiterung

Die Certificate Extensions werden in der jeweils aktuellen Fassung der CP definiert.

7.4 Profile für Sperrlisten

Die Anforderungen an die Sperrlisten (Certification Revocation List, CRL)-Profile werden in der jeweils aktuellen Fassung der CP definiert.

7.5 Profile für OCSP Dienste

In der PKI werden keine OCSP-Dienste eingesetzt.

8 Überprüfung und andere Bewertungen

In diesem Kapitel werden die Überprüfungen definiert, die den Teilnehmern der PKI als Auflage im Rahmen ihrer Antragszeit und Nutzung der PKI auferlegt werden.

8.1 Inhalte, Häufigkeit und Methodik

8.1.1 Beantragung Teilnahme an PKI

Folgende Anforderungen MÜSSEN bei Beantragung der Teilnahme an der PKI erfüllt werden. Teilweise sind dazu vorab die aufgeführten Nachweise zu erbringen.

Antrag für Teilnahme als	Nachweis	Überprüfung der Nachweise	Wichtung
Sub-CA	ISO27001-Zertifizierung der Sub-CA	ISO27001 Lead Auditor	Voraussetzung
	Signierte E-Mail der Root-CA über erfolgreiche Tests	Prüfer der Root-CA	
EZT	Verpflichtungserklärung des Teilnehmers, dass die Anforderungen dieser CP an einen EZT in der Betriebsumgebung des Teilnehmers umgesetzt werden.	Mitarbeiter der RA der entsprechenden Sub-CA	Voraussetzung

Tabelle 11 Anforderungen für die Teilnahme an der PKI

8.1.2 Wirkbetrieb

Die vorausgesetzten Nachweise/Zertifizierungen MÜSSEN im Wirkbetrieb auf Basis des jeweiligen Prüf-/Zertifizierungsschemas aufrechterhalten werden.

Sollte eine Zertifizierung nicht mehr gültig sein, so MUSS dies der zuständigen CA umgehend mitgeteilt werden.

Sollte eine Sub-CA eine geänderte Version ihrer Certificate Policy veröffentlichen, so MUSS die Root hierüber über einen der benannten Ansprechpartner mittels E-Mail informiert werden.

8.2 Reaktionen auf identifizierte Vorfälle

Die Reaktionen auf identifizierte Vorfälle sind in mittels der definierten Meldepflichten abgedeckt.

9 Sonstige finanzielle und rechtliche Regelungen

9.1 Preise

An die Nutzer von Zertifikaten werden keine separierten preislichen Anforderungen gestellt.

9.2 Finanzielle Zuständigkeiten

Die Root-CA sowie die Sub-CAs obliegen der finanziellen Zuständigkeit des Abrechnungszentrum Emmendingen und damit den entsprechenden Regelungen innerhalb des Abrechnungszentrum Emmendingens.

Anhang A: Namensschema

Die Common Names (CN) der verschiedenen PKI Teilnehmer MÜSSEN folgendem Schema entsprechen:

‘<org>.<function>[.<extension>]‘

Durch die Registrierungsprozesse MUSS von den CAs sichergestellt werden, dass die PKI-Teilnehmer die Common Names (Funktionskennzeichnung ‘<function>‘) entsprechend ihrer PKI-Rolle zugewiesen bekommen.

Eine Sub-CA MUSS sicherstellen, dass ein Common Name in Kombination mit der Sequenznummer unter dem Issuer Common Name der Sub-CA bei Endnutzer-Zertifikaten (bzw. bei einem Zertifikatstripel) aus - schließlich einmal vergeben wird, um die Eindeutigkeit dieser Zertifikate in der PKI zu gewährleisten. Des Weiteren MUSS die Root sicherstellen, dass jede Sub-CA einen anderen Common Name erhält.

Die folgende Tabelle beschreibt die Bestandteile der CN für die Teilnehmer der PKI:

Namensteil	Bedeutung	Länge, Kodierung, Ausnahmen
<org>	Kürzel der Identität/Organisation	Länge max. 48 Zeichen, erstes Zeichen muss ein Buchstabe oder eine Ziffer sein.
<function>	Funktionskennzeichnung innerhalb der PKI	Länge max. 4 Zeichen. Feste Werte: CA, SCA, EZT
<extension>	Erweiterung, zusätzliche Informationen	Länge max. 10 Zeichen. Optional, z.B. für leichteres Auffinden in Listen. Zwingend vorgegebene Werte bei CA‘s gemäß Tabelle 18 (Root-CA) und 22 (Sub-CA).

Tabelle 12 Namensschema (Kodierung Common Name)

Grundsätzliche Festlegungen:

- Die Länge des CN ist auf 64 Zeichen begrenzt.
- Die Kodierung ist ‘Printable String‘.
- Die zulässigen Zeichen sind: „0...9“, „a...z“, „A...Z“, „-“ (keine Leerzeichen).
- Der Punkt („.“) ist ausschließlich als Trennzeichen zwischen den Namensteilen zulässig und MUSS bei Vorhandensein im Namen des Zertifikatsinhabers weggelassen oder durch ein „-“ ersetzt werden.
- Die Leserichtung ist von links nach rechts (parsen, z.B. nach dem ersten Punkt immer ‘<function>‘).
- Endnutzer (EZT) KÖNNEN auf Basis der <extension> eine bessere Unterscheidbarkeit der von Ihnen genutzten Zertifikate herbeiführen. In dieser <extension> kann, nach der einmaligen Registrierung, eine individuelle Nummerierung oder z.B. ein Bezug auf einen Verwaltungsbereich (Kürzel Ortsangabe etc.) erfolgen.

Eine Erweiterung des Namensschemas ist möglich durch die Nutzung/Vorgabe weiterer Funktionsbezeichnungen und die Flexibilität der Nutzung der zusätzlichen Informationen in der optionalen Erweiterung.

Das Kürzel der Identität (<org>) wird durch den Zertifikatsinhaber festgelegt und sollte:

- kurz,
- sprechend (Identität erkennbar) und
- eindeutig

sein.

Ausnahmen bzw. Festlegungen für das Kürzel der Identität (<org>):

Root-CA: „ARZ-Root“

Die Zertifikate der Wirkumgebung haben das in den folgenden Tabellen angegebene Namensschema.

Root-CA

Die Zertifikate der Root-CA haben folgendes Namensschema:

C(Root) und Link-C(Root):

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„ARZ-Root.CA“	Name der Root-CA
organisation	O	mandatory	„PKI“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	„DE“	Ländercode
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer des Zertifikats im Bereich von 1 bis 2^{31}-1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.

Tabelle 13 Namensschema Zertifikat C(Root) und Link-C(Root)

C_{CRL-S}(Root)

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„ARZ-Root.CA.CRL-S“	Kennzeichnung als CRL-Signer
organisation	O	mandatory	„PKI“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	„DE“	Ländercode

Tabelle 14 Namensschema Zertifikat C_{CRL-S}(Root)

C_{TLS-S}(Root)

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„ARZ-Root.CA.TLS-S“	Kennzeichnung als TLS-Signer
organisation	O	mandatory	„PKI“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	„DE“	Ländercode
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer des Zertifikats im Bereich von 1 bis 2^{31}-1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.

Tabelle 15 Namensschema Zertifikat C_{TLS-S}(Root)

C_{TLS}(Root)

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„ARZ-Root.CA.TLS“	Kennzeichnung als TLS-Zertifikat der Root
organisation	O	mandatory	„PKI“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	„DE“	Ländercode
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer des Zertifikats im Bereich von 1 bis 2^{31}-1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.

Tabelle 16 Namensschema Zertifikat C_{TLS}(Root)

Sub-CA

Sub-CAs haben folgendes Namensschema:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<org>.CA“	Eindeutiger Name der Sub-CA.
organisation	O	mandatory	„PKI“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	<LC>	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer des Zertifikats im Bereich von 1 bis 2^{31}-1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.
street	street	optional	„<Straße>“	Straße der Sub-CA

postal code	postal code	optional	„<PLZ>“	Postleitzahl der Sub-CA
locality	L	optional	„<Ortsname>“	Ortsname des Sub-CA-Inhaberstandortes
state	ST	optional	„<Bundesland>“	Bundesland des Sub-CA-Inhaberstandortes

Tabelle 17 Namensschema der Sub-CA-Zertifikate

Bei den TLS-Zertifikaten der Sub-CA MUSS der common name, wie in folgenden Tabelle definiert ergänzt werden. Die Unterscheidung, ob das Zertifikat von der Root oder der Sub-CA selbst ausgestellt wurde, erfolgt über den Issuer-DN im Zertifikat.

Zertifikat	Wert	Erläuterung
$C_{TLS,Root}$(Sub-CA)	„<org>.CA.TLS“	Kennzeichnung als TLS-Zertifikat der Sub-CA
C_{TLS}(Sub-CA)	„<org>.CA.TLS“	Kennzeichnung als TLS-Zertifikat der Sub-CA

Tabelle 18 Erweiterung Common Name: TLS-Zertifikate Sub-CA

EZT

EZTs haben folgendes Namensschema:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<org>.EZT[.<extension>]“	Eindeutiger Name der Organisation
organisation	O	mandatory	„PKI“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	<LC>	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer des Zertifikats im Bereich von 1 bis 2^{31}-1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.
street	street	optional	„<Straße>“	Straße des Zertifikatsinhabers
postal code	postal code	optional	„<PLZ>“	Postleitzahl des Zertifikatsinhabers
locality	L	optional	„<Ortsname>“	Ortsname des Zertifikatsinhabers
state	ST	optional	„<Bundesland>“	Bundesland des Zertifikatsinhabers

Tabelle 19 Namensschema der EZT-Zertifikate

Alternativnamen

Die Zertifikatserweiterungen (extensions) SubjectAltNames und IssuerAltName MÜSSEN gemäß der folgenden Tabellen (Tabelle 20und Tabelle 21) genutzt werden.

SubjectAltNames

Die Belegung der Extension SubjectAltNames (Extension-ID (OID): 2.5.29.17) ist wie folgt:

Zertifikat	Rfc822Name	dNSName	uniformResourceIdentifier
C(Root)	eine Kontakt E-Mail-Adresse	Entfällt	Zugehörige Webseite
C_{CRL-S}(Root)		Entfällt	
C_{TLS-S}(Root)		Entfällt	
C_{TLS}(Root)		Domain Name (TLS-Server-Zertifikat)	
$C_{TLS,Root}$(Sub-CA)			
C(Sub-CA)		Entfällt	
C_{TLS}(Sub-CA)		Domain Name (TLS-Server-Zertifikat)	Optional: Zugehörige Webseite
		Domain Name (ausschließlich bei einem TLS-Server-Zertifikat, siehe nachfolgende Anforderungen)	

Tabelle 20 Belegung Extension SubjectAltNames für CAs und Endnutzer

Bei einem TLS-Server-Zertifikat, welches über die Extension ExtendedKeyUsage mit dem Wert TLS-Web- Server-Authentifikation (1.3.6.1.5.5.7.3.1) verfügt, MUSS der zugehörige Domain Name in der Extension SubjectAltNames angegeben werden.

Falls notwendig, ist es möglich mehrere Domain Name aufzunehmen, mit einer Obergrenze von 20 Einträgen.

Zertifikate DÜRFEN KEINE Wildcards im SubjectAltName enthalten.

IssuerAltName

Die Belegung der Extension IssuerAltName (Extension-ID (OID): 2.5.29.18) ist wie folgt:

Zertifikat	Inhalt
C(Root)	Entsprechend der Extension SubjectAltNames in C(Root) (s. Tabelle 28)
C_{CRL-S}(Root)	
C_{TLS-S}(Root)	
C(Sub-CA)	
C_{TLS}(Root)	Entsprechend der Extension SubjectAltNames in C_{TLS-S}(Root) (s. Tabelle 28)
$C_{TLS,Root}$(Sub-CA)	
C_{TLS}(Sub-CA)	Entsprechend der Extension SubjectAltNames in C(Sub-CA) (s. Tabelle 28)

Tabelle 21 Belegung Extension IssuerAltName für CAs und Endnutzer

Archivierung

Die folgende Tabelle gibt die Archivierungszeiträume für die unterschiedlichen Zertifikate der PKI Teilnehmer wieder. Die Speicherung bzw. auch die Bereitstellung der Zertifikate KANN in dem Index-Verzeichnis der Sub-CA erfolgen, wobei die anderen Teilnehmer von der eigenverantwortlichen Speicherung der Zertifikate nicht befreit werden.

Teilnehmer	Archivierungsort	Zertifikatstyp	Archivierungsdauer
Root-CA	Zertifikatsspeicher	C(Root)	Zertifikatslaufzeit + 10 ½ Jahre
		LinkC(Root)	
		C_{CLR-S}(Root)	
		C_{TLS-S}(Root)	
		C_{TLS}(Root)	
Sub-CA	Zertifikatsspeicher	C(Sub-CA)	Zertifikatslaufzeit + 10 ½ Jahre
		C_{TLS}(Sub-CA)	
EZT	Zertifikatsspeicher	C_{TLS}(EZT)	Zertifikatslaufzeit + 2 ½ Jahre
		C_{Enc}(EZT)	
		C_{Sig}(EZT)	

Tabelle 22 Archivierung öffentlicher Schlüssel

Definitionen

Begriff	Beschreibung
Ansprechpartner	Der Ansprechpartner (auch ASP oder Vertreter genannt) ist im Rahmen der operativen Tätigkeit der Vertreter des Unternehmens in Richtung der CA- Instanz und darf in dessen Namen die Entscheidungen treffen bzw. die Anträge autorisieren.
Antragsteller	Der Antragsteller im Sinne dieses Dokumentes ist das Unternehmen, welches die Zertifikate für den Betrieb einer Sub-CA anfordert.
Vier-Augen-Prinzip	Parallele Gegenkontrolle durch eine zweite Person bei der Durchführung eines Vorgangs. Die eindeutige Identifikation und Rolle der teilnehmenden Mitarbeiter MUSS protokolliert werden. Das Vier-Augen-Prinzip KANN organisatorisch so umgesetzt werden, dass bei diesem Prozess zwei unterschiedliche Personen beteiligt sein MÜSSEN, die nicht zeitgleich gemeinsam am gleichen Ort agieren MÜSSEN.
Schlüsselmanagement	Verwaltung von Schlüsseln (insbesondere Erzeugung, Speicherung und Löschung bzw. Zerstörung von Schlüsseln)
Hinterlegung von Schlüsseln	Sichere Verwahrung einer Kopie eines Schlüssels an einem Zweitort.
Zerstörung von Schlüsseln	Zerstörung des Schlüssels durch einen sicheren Löschmechanismus im Kryptografiemodul. Dieser wird i.d.R. durch ein Überschreiben mit einem vorgegebenen Wert oder durch das interne dauerhafte Sperren aller Zugriffe auf den Schlüssel realisiert. Verfügt das Kryptografiemodul nicht über einen entsprechen Löschmechanismus, muss eine unwiederherstellbare mechanische Zerstörung erfolgen.
PKI-Rolle	Die PKI-Rolle beschreibt die Funktionsklasse eines PKI-Teilnehmers in der PKI. Folgende PKI-Rollen sind in der PKI vorhanden: EZT, Sub-CA und Root-CA. Ein PKI-Teilnehmer ist eine Instanz seiner PKI-Rolle.
Sequenznummer	SERIAL NUMBER des Distinguished Name, siehe Anhang A
Serialnumber	serialNumber Feld des Zertifikats

Tabelle 23 Definitionen

Stichwort- und Abkürzungsverzeichnis

Abkürzung	Begriff
ASP	Ansprechpartner (des Unternehmens)
CA	Certificate Authority
CC	Common Criteria
CER	Canonical Encoding Rules (Format zur Zertifikatscodierung)
CLS	Controllable Local Systems

CN	Common Name
CP	Certificate Policy
CPS	Certificate Practise Statement
CRL	Certificate Revocation List (Zertifikatssperrliste)
DRG	(Funktionsklasse für Zufallsgeneratoren)
DN	Distinguished Name
EZT	Externe Zertifizierungsteilnehmer
ENC	Encryption / Verschlüsselung
HAN	Home Area Network (Heimnetz)
HSM	Hardware Sicherheitsmodul
ISMS	Information Security Management System
ISO	International Organization of Standardization
KEK	Key Encyption Key
KM	Krypto Modul
NTG	hybride deterministische Zufallszahlgeneratoren (Funktionsklasse für Zufallsgeneratoren)
OCSP	Online Certificate Status Protocol
PIN	Personal Identifikation Number
PKI	Public Key Infrastructure
PP	Protection Profile
PTG	hybride physikalische Zufallszahlgeneratoren (Funktionsklasse für Zufallsgeneratoren)
RA	Registration Authority
SHA	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Mail Extension
PKI	– Public Key Infrastructure
TLS	Transport Layer Security (Protokoll zur Verschlüsselung einer Datenübertragung)
WAN	Wide Area Network (Weitverkehrsnetz)
X.509	ITU-T-Standard für eine Public-Key-Infrastruktur

Tabelle 24 Stichwort und Abkürzungsverzeichnis