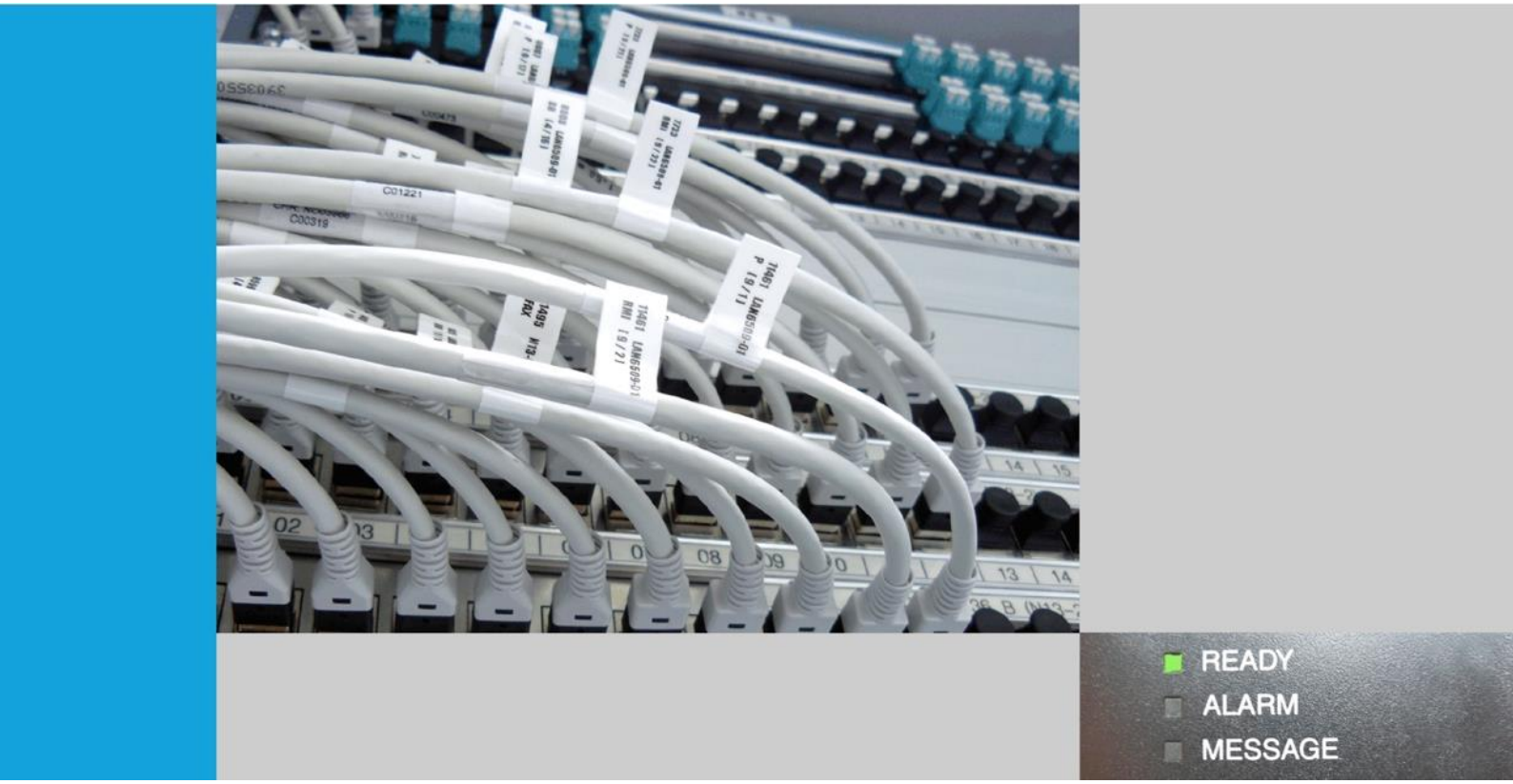
Landesamt für Digitalisierung,
Breitband und Vermessung

IT-Dienstleistungszentrum des Freistaats Bayern



Zertifizierungsrichtlinie der Public Key Infrastructure der Bayerischen Verwaltung

für die
X.509-Zertifizierungshierarchie Bayern-PKI

Bearbeitung:
Kerstin Ehrhardt

München, den 11. März 2021

Dokumentenentwicklung

Version	Datum	Bearbeiter	Beschreibung, QS-Maßnahme	Status *s. u.
1.0	12.04.19	Ehrhardt	Dokument erstellt	freigegeben
1.1	21.05.19	Ehrhardt	Änderungen an Kapiteln 3.1.2, 3.1.4, 3.1.5, 4.9.1, 4.9.2, 4.9.3, 4.9.9, 4.9.10, 4.9.13-16, 4.10, 6.1.1, 6.2.9 Neu: 4.2.4	In Bearbeitung
1.2	11.07.19	Ehrhardt	Nach Review kleinere Änderungen	freigegeben
1.3	11.03.21	Hohmuth, Ehrhardt	Inkonsistente Verwendung der Begriffe „Server“ und „IT-Prozess“ aufgelöst	freigegeben

* zu verwenden sind: in Bearbeitung, vorgelegt, freigegeben

Inhaltsverzeichnis

1 Einführung

Das Bayerische Landesamt für Digitalisierung, Breitband und Vermessung (LDBV) betreibt im Auftrag des Bayerischen Staatsministeriums der Finanzen zentrale Komponenten und Dienste des Bayerischen Behördennetzes (BYBN). Das BYBN ist ein auf Internet-Techniken basierendes geschlossenes Netz (Intranet) für alle staatlichen und kommunalen Behörden im Freistaat Bayern. Zu den vom LDBV bereitgestellten Diensten zählt eine Public Key Infrastructure (PKI).

Die PKI stellt Zertifikate für natürliche Personen, juristische Personen, Personengruppen, Funktionen und automatisierte IT-Prozesse aus. Den Teilnehmern wird die PKI angeboten, um die Vertraulichkeit, Integrität und Verbindlichkeit von Daten bzw. Nachrichten zu gewährleisten. Teilnehmer sind Mitarbeiter der staatlichen und kommunalen Verwaltungen in Bayern sowie in Ausnahmefällen vertrauenswürdige Dritte.

Die vom LDBV betriebene PKI besteht aus mehreren eigenständigen Zertifizierungshierarchien. Gegenstand dieser Zertifizierungsrichtlinie ist die Zertifizierungshierarchie, die X509-Zertifikate für E-Mailsignatur, -verschlüsselung, Authentifizierung, Dokumentensignatur, Code-Signing und automatisierte IT-Prozesse innerhalb der Bayerischen Verwaltung ausstellt. Sie stellt eine Nachfolgelösung der Bayerischen Verwaltungs-PKI, die früher unterhalb der vom BSI betriebenen Deutschen Verwaltungs-PKI betrieben wurde, dar. Dienstleistungen, die nicht durch die Richtlinien der Bayern-PKI abgedeckt sind, werden in eigenständigen Zertifizierungshierarchien angeboten, die jedoch nicht Gegenstand dieser Zertifizierungsrichtlinie sind.

Die von der Bayern-PKI ausgegebenen Zertifikate genügen den Anforderungen für fortgeschrittene elektronische Signaturen.

1.1 Überblick

1.1.1 Aufbau und Zweck des Dokumentes

Mit diesem Dokument werden die Anforderungen für die Ausstellung und Sperrung von Zertifikaten nach den Standards X.509 festgeschrieben. Dieses Dokument beschreibt die Vorgaben für das Sicherheitsniveau der Bayern-PKI und soll dem Leser ein allgemeines Verständnis der Bayern-PKI ermöglichen.

Die technischen Maßnahmen und Prozesse sind detailliert in den zugehörigen Regelungen für den Zertifizierungsbetrieb [1] beschrieben. Die Zertifizierungsrichtlinie und die Regelungen für den Zertifizierungsbetrieb orientieren sich an den Vorgaben aus RFC 3647.

1.1.2 Aufbau der Bayern-PKI

Die PKI der bayerischen Verwaltung besteht aus mehreren, voneinander unabhängigen Zertifizierungshierarchien nach X.509. Für die einzelnen Hierarchien gelten unterschiedliche Anforderungen, die in jeweils eigenständigen Zertifizierungsrichtlinien beschrieben werden.

Diese Zertifizierungsrichtlinie befasst sich mit den Anforderungen an die Bayern-PKI.

1.2 Name und Identifikation des Dokumentes

Name:	Zertifizierungsrichtlinie der Bayern-PKI
Version:	1.3
Datum:	11.03.2021
Identifier:	1.3.6.1.4.1.19266.1.2.4

1.3 PKI Teilnehmer

1.3.1 Zertifizierungsstellen

Die Zertifizierungsstellen geben Zertifikate für Zertifizierungsstellen oder Zertifikatsnehmer aus. Die Wurzelzertifizierungsstelle der Bayern-PKI wird vom LDBV/ IT-DLZ betrieben. Für die Bayern-PKI ist eine maximal dreistufige PKI-Hierarchie vorgegeben. In dieser Hierarchie bilden die Zertifikatsnehmer die unterste Stufe und die Wurzelzertifizierungsstelle die oberste Stufe.

Alle Zertifizierungsstellen der Bayern-PKI werden vom LDBV betrieben.
Die Wurzelzertifizierungsstelle zertifiziert ausschließlich nachgeordnete Zertifizierungsstellen. Die nachgeordneten Zertifizierungsstellen stellen ausschließlich Endstellenzertifikate aus.

1.3.2 Registrierungsstellen

Für die Bayern-PKI gibt es eine Wurzelregistrierungsstelle (übergeordnete Registrierungsstelle). Diese registriert weitere Registrierungsstellen. Zertifikatsnehmer werden durch die Wurzelregistrierungsstelle nicht registriert. Die Wurzelregistrierungsstelle wird vom LDBV betrieben.

Es gibt ein Netz von Registrierungsstellen zur Sicherstellung der Identität von Zertifikatsnehmern sowie zur Überprüfung von Zuständigkeits- oder Vertretungsnachweisen. Die Registrierungsstellen sind gegenüber den Zertifizierungsstellen für die Richtigkeit der erfassten Daten verantwortlich. Die Registrierungsstellen sichern gegenüber dem LDBV die Einhaltung dieser Richtlinie und der zugehörigen Regelungen für den Zertifizierungsbetrieb schriftlich in einer Selbsterklärung zu.

1.3.3 Zertifikatsnehmer

Zertifikate und Schlüssel werden für die staatliche und kommunale Verwaltung in Bayern ausgegeben. In Ausnahmefällen können Zertifikate und Schlüssel auch an natürliche Personen (vertrauenswürdige Dritte) außerhalb der staatlichen und kommunalen Verwaltungen in Bayern ausgegeben werden, wenn staatliche oder kommunale Behörden ein berechtigtes Interesse nachweisen, mit diesen gesichert über das Internet zu kommunizieren.

Zertifikatsnehmer können sein:

- natürliche Personen,
- juristische Personen,
- Personengruppen (z. B. Projektteam, Arbeitsgruppe),
- Funktionen (z.B. Poststelle, Registrierungsstelle; Funktion, die durch einen Mitarbeiter ausgefüllt wird),
- Automatisierte IT-Prozesse (z.B. Zertifizierungsstelle, Serverprozesse mit Signatur, SSL-Server, Workstations, Mobile Device Management Systeme).

Zertifikatsverantwortliche:

Für Zertifikate oder Schlüssel muss immer eine einzelne natürliche Person verantwortlich sein (im Folgenden als Zertifikatsverantwortlicher bezeichnet). Dies gilt, wenn die Zertifikate oder Schlüssel für ihre eigene Person ausgestellt wurden. Dies gilt auch, wenn die Zertifikate und Schlüssel für eine juristische Person, Personengruppe, Funktion oder einen automatisierten IT-Prozess ausgestellt wurden, wofür sie einen entsprechenden Zuständigkeits- oder Vertretungsnachweis beigebracht hat.

1.3.4 Zertifikatsprüfer

Zertifikatsprüfer überprüfen anhand eines Zertifikates der Bayern-PKI die Authentizität einer Person, einer Personengruppe, einer Funktion oder eines automatisierten IT-Prozesses. Für

die Überprüfung werden das Zertifikat selber, die in der Zertifizierungshierarchie übergeordneten Zertifikate, die Gültigkeit sowie die zur Verfügung stehenden Sperrinformationen ausgewertet. Ein Zertifikatsprüfer kann gleichzeitig Zertifikatsnehmer sein.

1.3.5 Andere PKI Teilnehmer

Weitere Teilnehmer sind Dienstleister im Auftrag der PKI (z. B. Betreiber von Verzeichnisdiensten).

1.4 Verwendungszweck der Zertifikate

1.4.1 Geeignete Verwendungszwecke innerhalb der Bayern-PKI

Die Schlüssel und Zertifikate dürfen zur Erzeugung von fortgeschrittenen Signaturen, zur Authentisierung, zur Ver-/ Entschlüsselung von Daten oder für automatisierte IT-Prozesse eingesetzt werden.

Die Schlüssel und Zertifikate dürfen nur für den Dienstgebrauch eingesetzt werden.

1.4.2 Verbotene Verwendungszwecke innerhalb der Bayern-PKI

Private Nutzung der Schlüssel und Zertifikate ist nicht gestattet.

1.5 Verwaltung der Richtlinien

1.5.1 Änderungsmanagement

Die vorliegende Zertifizierungsrichtlinie sowie die Regelungen zum Zertifizierungsbetrieb werden durch das LDBV verwaltet. Änderungen an der Zertifizierungsrichtlinie werden im Abschnitt Änderungshistorie zu Beginn des Dokumentes protokolliert.

1.5.2 Ansprechstelle

Bayerisches Landesamt für Digitalisierung, Breitband und Vermessung
- Trustcenter -
St.-Martin-Straße 47
81541 München

Telefon: 089/2119-4924
Fax: 089/2119-14924
E-Mail: trustcenter@ldbv.bayern.de

1.5.3 Eignungsprüfer für Regelungen zum Zertifizierungsbetrieb gemäß Zertifizierungsrichtlinie

Keine Festlegung.

1.5.4 Verfahren zur Anerkennung von Regelungen zum Zertifizierungsbetrieb

Eine Kopplung zweier Zertifizierungsinfrastrukturen (Cross-Zertifizierung) ist nicht vorgesehen.

1.6 Definitionen und Abkürzungen

Siehe Glossar (Kapitel 10).

2 Veröffentlichungen und Verzeichnisdienst

2.1 Verzeichnisdienst

Die Zertifizierungsstellen stellen die von ihnen ausgestellten Zertifikate und Sperrinformationen in das LDAP-Verzeichnis des IT-DLZ ein. Der Abruf der Informationen erfolgt über LDAPv3 gemäß RFC 2251 ohne Security-Layer (SSL oder TLS).

Die Zertifizierungsstellen- und Benutzerzertifikate sollen im Verzeichnisdienst in dem durch den Namen des Zertifikatsinhabers festgelegten Knoten standardisiert abgelegt werden. Die Sperrliste soll im Verzeichnisdiensteintrag der Zertifizierungsstelle veröffentlicht werden. Sofern die Zertifikate der Zertifizierungsstellen und Sperrlisten an anderer Stelle publiziert werden sollen, muss der Verweis auf diesen Ort der Publikation in die ausgestellten Zertifikate aufgenommen werden.

2.2 Veröffentlichung der Informationen

Die innerhalb der Bayern-PKI ausgestellten Zertifikate von Zertifikatsnehmern sollen in einem nur innerhalb des BYBN zugänglichen Verzeichnisdienst veröffentlicht werden. Der Zertifikatsverantwortliche wird bei der Beantragung eines Zertifikats auf die Veröffentlichung hingewiesen. Zertifikate von Zertifizierungsstellen, Informationen zur Überprüfung der Gültigkeit aller Zertifikate sowie Zertifikate von Zertifikatsnehmern, die einer Veröffentlichung im Internet ausdrücklich zugestimmt haben, sollen im Internet veröffentlicht werden.

Den Zertifikatsnehmern und -prüfern sollen folgende Informationen zur Verfügung gestellt werden:

- Verweis auf Wurzelzertifikat und dessen Fingerabdruck
- Für jede Zertifizierungsstelle ihr Zertifikat und dessen Fingerabdruck
- Zertifizierungsrichtlinie
- Aktuelle Sperrlisten
- Zertifikate der Zertifikatsnehmer (BYBN-intern und nach Zustimmung der Benutzer auch im Internet)

2.3 Aktualisierung der Informationen

Zertifikate und Sperrlisten sollen unmittelbar nach ihrer Ausstellung im Verzeichnisdienst publiziert werden.

2.4 Zugangskontrolle zu den Informationen

Der lesende Zugriff auf die unter 2.1 und 2.2 genannten Informationen muss ohne Anmeldung erfolgen können. Der schreibende Zugriff ist auf berechtigte Personen beschränkt.

3 Identifizierung und Authentifizierung

3.1 Namen

Die verwendeten Namen müssen den Vorgaben des Standards X.509 entsprechen, d.h. das Attribut „issuer Distinguished Name (DName)“ im Zertifikat muss identisch zum Attribut „subject DName“ im Zertifikat der ausstellenden Zertifizierungsstelle sein, um den Aufbau des Zertifikatspfades zu ermöglichen.

Es wurde ein eindeutiger Namensraum festgelegt:

- C = DE,
- O = Freistaat Bayern.

Innerhalb der Bayern-PKI ist dieser Namensraum zu verwenden.

3.1.1 Namenstypen

Die folgenden Namenstypen können unterstützt werden:

- DName
- URI
- LDAP-Namen
- RFC-822 Name

Zertifikatsinhaber und Zertifikatsaussteller müssen einen eindeutigen DName zugewiesen bekommen. Die LDAP-Namen müssen auf die Einträge verweisen, wo das Zertifikat und die Sperrliste der Bayern-PKI-CA im LDAP-Verzeichnis veröffentlicht sind. Die HTTP URIs sollen die von extern erreichbaren Adressen kennzeichnen, wo das Zertifikat und die Sperrliste der Bayern-PKI-CA zu finden sind. Der RFC-822-Name soll die E-Mail-Adresse des Zertifikatsinhabers beinhalten.

Beim Namenstyp DName sind folgende Festlegungen zu beachten:

- Im Attribut subject eines Zertifikats für Zertifizierungsstellen müssen im DName die Bestandteile „countryName“ und „organizationName“ enthalten sein.
- Im Attribut subject eines Zertifikats für Zertifikatsnehmer müssen im DName die Bestandteile „commonName“ (cn), „organizationalUnitName“ (ou), „organizationName“ (o) und „CountryName“ (c) enthalten sein.
- Bei Zertifikaten für Gruppen oder Funktionen muss aus dem Subject-DName eindeutig hervorgehen, dass es sich bei diesem Teilnehmer um eine Gruppe oder Funktion handelt. Dazu wird dem Namen ein „FKT:“ vorangestellt.

3.1.2 Aussagekraft von Namen

Namen müssen aussagekräftig eindeutig und einmalig sein, um die Zertifikatsinhaber identifizieren zu können. Folgende Regelungen gelten:

- Zertifikate für natürliche oder juristische Personen sind auf den Namen der Person auszustellen.
- Zertifikate für Personengruppen oder Funktionen dürfen nicht auf die Namen von natürlichen oder juristischen Personen ausgestellt werden und müssen sich deutlich von Zertifikaten für natürliche oder juristische Personen unterscheiden.
- Bei Zertifikaten für natürliche Personen, juristische Personen, Personengruppen oder Funktionen muss aus dem Namen, auf den das Zertifikat ausgestellt wurde, die Dienststelle eindeutig hervorgehen. Bei vertrauenswürdigen Dritten muss der Firmenname eindeutig hervorgehen.

- Zertifikate für automatisierte IT-Prozesse dürfen nicht auf die Namen von natürlichen oder juristischen Personen ausgestellt werden.
- Der Name des IT-Prozesses muss eindeutig hervorgehen.
- Wildcard-Zertifikate sind unter bestimmten Voraussetzungen erlaubt (vgl. 6.1.1 und 6.2).

Die Einhaltung der Namenskonventionen ist von der jeweils zuständigen Registrierungsstelle sicherzustellen.

3.1.3 Anonyme und Pseudonyme

Zertifikate der Bayern-PKI werden nur für dienstliche Zwecke ausgestellt. Daher sind innerhalb der Bayern-PKI Anonymität und Pseudonymität im Namen des Zertifikates nicht erlaubt.

3.1.4 Namensinterpretation

Wenn ein Name im Zertifikat vom Namenstyp RFC-822 ist, so muss dieser die E-Mail-Adresse des Zertifikatsnehmers enthalten.

Distinguished Names in Zertifikaten sollen entsprechend dem Standard X.500 und der ASN.1-Syntax interpretiert werden. Relevant hierfür sind die RFC's 2253 und 2616.

3.1.5 Eindeutigkeit von Namen

Die Eindeutigkeit von Namen muss von der Zertifizierungsstelle gewährleistet werden. Ein Wildcard-Zertifikat darf für mehrere Instanzen genutzt werden.

3.1.6 Wiedererkennung, Authentifizierung und Funktion von Warenzeichen

Zertifikatsnehmer dürfen keine Namen in ihren Zertifikaten verwenden, die Warenzeichen oder Markennamen verletzen. Die Bayern-PKI ist bei der Ausstellung von Zertifikaten nicht dafür verantwortlich, eingetragene Warenzeichen oder Markennamen zu überprüfen.

3.2 Identitätsüberprüfung bei Neuanträgen

3.2.1 Nachweis des Besitzes des privaten Schlüssels

Wird der private Schlüssel von der Zertifizierungsstelle erzeugt, muss die Zertifizierungsstelle den privaten Schlüssel mit einem geeigneten Passwort für den Transport verschlüsseln. Es muss sichergestellt werden, dass nur der Zertifikatsverantwortliche das Passwort erhalten kann. Die Übermittlung des privaten Schlüssels und des zugehörigen Passworts muss auf getrennten Wegen erfolgen.

Wird der private Schlüssel vom Zertifikatsnehmer erzeugt, so muss der Zertifikatsverantwortliche den Besitz des privaten Schlüssels gegenüber der Zertifizierungsstelle versichern – zum Beispiel durch eine elektronische Signatur des Zertifikatsantrags, wenn er den zugehörigen öffentlichen Schlüssel bei der Zertifizierungsstelle zur Zertifizierung vorlegt.

3.2.2 Authentifikation von organisatorischen Einheiten (juristischen Personen, Personengruppen und Funktionen)

Registrierungsstellen müssen sich als Funktion bei der Wurzelregistrierungsstelle registrieren.

Zertifikatsnehmer müssen sich bei einer der Wurzelregistrierungsstelle nachgeordneten Registrierungsstellen authentisieren.

Sollen Zertifikate auf juristische Personen, Personengruppen oder Funktionen automatisierte IT-Prozesse ausgestellt werden, so ist hierfür ein Zertifikatsverantwortlicher von der für den Einsatz der Zertifikate verantwortlichen Stelle gegenüber der Registrierungsstelle zu benennen. Dieser Zertifikatsverantwortliche entspricht rechtlich einem Zertifikatsnehmer und muss

von der Registrierungsstelle bzw. der Wurzelregistrierungsstelle gemäß den Regelungen aus Kapitel 3.2.3 identifiziert werden. Außerdem muss die Registrierungsstelle die für die Zertifikatserstellung notwendigen Daten überprüfen.

3.2.3 Authentifikation von natürlichen Personen

Die Überprüfung der Identität muss bei einer Registrierungsstelle erfolgen. Hierzu muss der Zertifikatsnehmer im Allgemeinen persönlich bei der Registrierungsstelle erscheinen. Die Registrierungsstelle muss die Identifizierung aufgrund eines Lichtbildausweises (Personalausweis, Reisepass, Behördenausweis) vornehmen. Außerdem muss die Registrierungsstelle die für die Zertifikatserstellung notwendigen Daten überprüfen.

Befindet sich die Registrierungsstelle und das für den Zertifikatsnehmer zuständige Personalbüro in derselben Behörde, kann auf das persönliche Erscheinen sowie auf die Prüfung eines Lichtbildausweises verzichtet werden und stattdessen die Identifizierung durch einen Datenabgleich mit dem Personalbüro erfolgen.

3.2.4 Nicht überprüfte Teilnehmerangaben

Keine Festlegung.

3.2.5 Überprüfung der Berechtigung

Für Zertifikate, die auf juristische Personen, Personengruppen, Funktionen und automatisierte IT-Prozesse ausgestellt werden, erfolgt keine Prüfung durch die Registrierungsstelle, in wie weit der benannte Zertifikatsverantwortliche tatsächlich für die Anfangs aufgelisteten Gruppen zuständig ist.

3.2.6 Interoperabilitätskriterien

Keine Festlegung.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Für die routinemäßige Zertifikatserneuerung ist keine erneute Identifizierung und Registrierung (Authentifizierung) nötig, da die Registrierungsdaten nach Zertifikatsablauf erhalten bleiben und bei Änderungen von der Registrierungsstelle angepasst werden. Somit wird die Vertrauenskette nicht gebrochen.

Bei zentraler Schlüsselerzeugung darf eine automatische Zertifikatserneuerung durchgeführt werden.

3.3.2 Zertifikatserneuerung nach einem Zertifikatswiderruf

Nach einem Zertifikatswiderruf muss ein Neuantrag gestellt werden. Eine erneute Identifizierung bei einer Registrierungsstelle ist nicht notwendig.

3.4 Identifizierung und Authentifizierung bei einem Widerruf

Ein Antrag auf Zertifikatswiderruf soll durch den Zertifikatsverantwortlichen nach Authentisierung erfolgen. Die Authentisierung kann entweder über die Anmeldung an einer Schnittstelle der Zertifizierungsstelle oder, bei telefonischer Sperrung, mit Hilfe seines Sperrpassworts durchgeführt werden. Alternativ soll der Zertifikatsverantwortliche den Antrag auf Zertifikatswiderruf auch bei der zuständigen Registrierungsstelle stellen können. Die Registrierungsstelle muss den Zertifikatsverantwortlichen entsprechend der Regelungen in 3.2.3 identifizieren.

Die Registrierungsstelle oder die Wurzelregistrierungsstelle soll in begründeten Fällen (z. B. bei Ausscheiden aus dem Amt, bei Verstößen gegen die Sicherheitsrichtlinie) auch ohne Antrag des Zertifikatsverantwortlichen Zertifikate widerrufen können.

4 Ablauforganisation

4.1 Zertifikatsantrag

4.1.1 Wer kann einen Zertifikatsantrag stellen

Jeder Antragsteller, der von einer Registrierungsstelle nach Kapitel 3.2.2 oder 3.2.3 identifiziert und authentifiziert wurde, darf Zertifikate beantragen.

4.1.2 Prozess und Verantwortung

Antragsteller beantragen ihre benötigten Zertifikate direkt bei der Zertifizierungsstelle. Diese stellt hierfür zwei Möglichkeiten zur Verfügung:

- eine Software basierte Schnittstelle oder
- eine native Windows Enrollment Schnittstelle (Microsoft Autoenrollment).

Mit der Identifizierung bei der zuständigen Registrierungsstelle erhält der Antragsteller einen Brief mit seinen persönlichen Zugangsdaten zu o.g. Schnittstelle. Außerdem enthält der Brief das persönliche Sperrkennwort, mit dem alle für den Zertifikatsnehmer ausgestellten Zertifikate gesperrt werden können.

Im Zuge der erstmaligen Anmeldung an der Schnittstelle muss der Antragsteller sein Zugangspasswort so abändern, dass es nur ihm bekannt ist. Der Antragsteller ist dafür verantwortlich, dass niemand seine persönlichen Anmeldedaten kennt, auch nicht die Registrierungsstellen-, Zertifizierungsstellen- oder andere Trustcenter-Mitarbeiter.

Über die Schnittstelle kann der Antragsteller persönliche Zertifikate beantragen, verlängern und widerrufen. Dem Antragsteller werden digitale Formulare angeboten, die er vollständig auszufüllen hat. Anschließend wird der Antrag auf elektronischem Weg an die Zertifizierungsstelle übermittelt.

Sollen Zertifikate auf juristische Personen, Personengruppen, Funktionen oder automatisierte IT-Prozesse beantragt werden, so stellt die Registrierungsstelle die dafür notwendigen Anträge dem authentisierten Zertifikatsverantwortlichen ebenfalls über die o.g. Schnittstelle bereit.

Mit der Antragstellung muss der Antragsteller die Zertifizierungsrichtlinien der Zertifizierungsstelle akzeptieren.

Von der Zertifizierungsstelle sollen Zertifikatsanträge mit zentraler oder mit dezentraler Schlüsselerzeugung bearbeitet werden.

Bei dezentraler Schlüsselerzeugung soll der Zertifikatsverantwortliche seine privaten Schlüssel selbst am eigenen PC erzeugen und dann einen Zertifikatsantrag stellen.

Bei zentraler Schlüsselerzeugung werden auch die privaten Schlüssel anhand der Antragsdaten in der Zertifizierungsstelle erzeugt und danach an den Zertifikatsverantwortlichen auf sicherem Wege ausgeliefert.

4.2 Bearbeitung von Zertifikatsanträgen

4.2.1 Durchführung von Identifikation und Authentifizierung

Vor der Antragstellung muss sich der Antragsteller bei einer Registrierungsstelle identifizieren. Die Registrierungsstelle pflegt die Antragstellerdaten in die Schnittstelle der Zertifizierungsstelle ein. Die Antragstellerdaten sind danach fest mit der Registrierungsstelle verknüpft. Die Registrierungsstelle ist entsprechend für die Richtigkeit der Daten verantwortlich. Dies gilt auch bei Änderungen an den Daten (z.B. E-Mail Adresse).

Nach erfolgter Identifikation erhält der Nutzer Authentifizierungsdaten, mit denen er sich anschließend an der Schnittstelle authentifizieren kann.

4.2.2 Annahme oder Ablehnung von Zertifikatsanfragen

Der vom Antragssteller gestellte Zertifikatsantrag soll direkt zur Zertifizierungsstelle übermittelt werden.

Die Zertifizierungsstelle soll den Antrag auf Vollständigkeit prüfen. Anschließend soll eine Überprüfung der Antragsdaten mit den Registrierungsdaten erfolgen, sodass der Antragsteller nur Zertifikate beantragen kann, die zuvor bei der Registrierungsstelle für ihn registriert wurden. Dies geschieht im Regelfall innerhalb der Schnittstelle während der Beantragung.

Sollte ein Antrag aus irgendeinem Grund abgelehnt werden, so muss dies dem Antragsteller unter Benennung der Gründe mitgeteilt werden.

4.2.3 Bearbeitungsdauer

Die Zertifikatsanträge müssen innerhalb von einem Werktag von der Zertifizierungsstelle bearbeitet werden.

4.2.4 Certificate Authority Authorisation (CAA)

Es erfolgt keine Prüfung von Certification Authority Authorisation (CAA) DNS Einträgen (RFC 6844).

4.3 Zertifikatserstellung

4.3.1 Aufgaben der Zertifizierungsstelle

Von der Zertifizierungsstelle sollen Zertifikatsanträge mit zentraler oder mit dezentraler Schlüsselerzeugung bearbeitet werden.

Bei zentraler Schlüsselerzeugung werden nach erfolgreicher Überprüfung des Zertifikatsantrags die privaten Schlüssel von der Zertifizierungsstelle erzeugt, die Zertifikate ausgestellt und sowohl das Schlüsselpaar als auch die Zertifikate inklusive der Zertifikate der Zertifizierungsstellen an den Zertifikatsverantwortlichen sicher ausgeliefert.

Bei dezentraler Schlüsselerzeugung stellt die Zertifizierungsstelle nach erfolgreicher Überprüfung des Zertifikatsantrags das Zertifikat aus und sendet dieses inklusive der Zertifikate der Zertifizierungsstellen an den Zertifikatsverantwortlichen zurück.

Die ordnungsgemäße Erstellung der beantragten Zertifikate und ggf. Schlüssel soll regelmäßig von einem Auditor überwacht werden.

4.3.2 Benachrichtigung des Antragstellers

Wird der Zertifikatsantrag abgelehnt, erhält der Antragsteller eine entsprechende Benachrichtigung. Anderenfalls erhält der Antragsteller das Zertifikat bzw. die PSE von der Zertifizierungsstelle der Bayern-PKI.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme des Zertifikates durch den Zertifikatsverantwortlichen

Nach Erhalt der Zertifikate (und ggf. der Schlüssel) muss der Zertifikatsverantwortliche dieses Material prüfen. Erfolgt kein Einspruch von Seiten des Zertifikatsverantwortlichen gilt das Zertifikat als akzeptiert.

Bei fehlerhaften Zertifikaten muss der Zertifikatsverantwortliche die Zertifikate widerrufen. Ein neues Zertifikat muss der Zertifikatsverantwortliche selbst beantragen (Zertifikatsneuantrag).

4.4.2 Zertifikatsveröffentlichung

Nach Erstellung der Zertifikate soll die Zertifizierungsstelle diese gemäß Abschnitt 2.2 in den vorgesehenen Verzeichnisdiensten veröffentlichen.

4.4.3 Benachrichtigung weiterer Instanzen

Es ist keine Benachrichtigung weiterer Beteiligter über eine Zertifikatsausstellung erforderlich.

4.5 Verwendung des Schlüsselpaares und des Zertifikates

4.5.1 Nutzung durch den Zertifikatsnehmer

Der Zertifikatsverantwortliche hat die Verantwortung für den sachgerechten und sicheren Gebrauch des Zertifikats und des zugehörigen privaten Schlüssel zu übernehmen. Bei Zertifikaten, die auf juristische Personen, Personengruppen und Funktionen ausgestellt werden, kann der Zertifikatsverantwortliche weiteren Personen den Zugriff auf den privaten Schlüssel ermöglichen.

Der Zertifikatsverantwortliche hat insbesondere die Aufgaben:

- bei Änderungen in den Zertifikatsdaten einen Widerruf zu beantragen,
- den privaten Schlüssel gesichert aufzubewahren,
- bei Abhandenkommen oder Kompromittierung des privaten Schlüssels einen Zertifikatswiderruf zu beantragen.

Der Zugriff auf den privaten Schlüssel muss gesichert (Passwort) erfolgen.

Der Zertifikatsnehmer darf seinen privaten Schlüssel und das zugehörige Zertifikat nur für die im Zertifikat benannten Verwendungszwecke einsetzen.

4.5.2 Nutzung durch Zertifikatsprüfer

Jeder Teilnehmer, der ein Zertifikat eines anderen Teilnehmers verwendet, muss sicherstellen, dass dieses Zertifikat nur innerhalb der im Zertifikat benannten Verwendungszwecke eingesetzt wird. Außerdem muss er bei jedem Einsatz die Gültigkeit des Zertifikates überprüfen.

4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (Re-Zertifizierung)

Eine Zertifikatserneuerung ohne Schlüsselerneuerung ist nicht zugelassen.

4.7 Schlüssel- und Zertifikatserneuerung (Re-key)

4.7.1 Bedingungen, Umstände, Gründe

Ein Antrag auf Schlüssel- und Zertifikatserneuerung darf nur bearbeitet werden, wenn

- bereits ein Zertifikat für diesen Zertifikatsnehmer ausgestellt wurde und
- dieses alte Zertifikat demnächst abläuft.

Wurde ein Zertifikat vor Ablauf seiner Gültigkeit widerrufen, so darf keine Zertifikatserneuerung erfolgen. Es muss ein Zertifikatsneuantrag gestellt werden.

4.7.2 Wer kann einen Antrag auf Schlüssel- und Zertifikatserneuerung stellen

Anträge auf Schlüssel- und Zertifikatserneuerung sollen vom Zertifikatsverantwortlichen gestellt werden. Bei zentraler Schlüsselerzeugung kann die Erneuerung auch automatisiert erfolgen.

4.7.3 Ablauf der Schlüsselerneuerung

Bei zentraler Schlüsselerzeugung soll der Zertifikatsverantwortliche sechs Wochen vor Ende der Laufzeit über die anstehende Zertifikatsverlängerung informiert werden. Sofern kein Zertifikatswiderruf erfolgt, soll danach der Zertifikatsverantwortliche 14 Tage vor Ende der Laufzeit die neuen Zertifikate und die dazugehörigen Schlüssel erhalten.

Bei dezentraler Schlüsselerzeugung entspricht die Zertifikatsverlängerung einem Zertifikatsneuantrag. Der Zertifikatsverantwortliche soll seine neuen privaten Schlüssel am eigenen PC erzeugen und dann einen digitalen Zertifikatsantrag bei der Zertifizierungsstelle der Bayerischen Verwaltungs-PKI einreichen. Es ist keine erneute Registrierung notwendig.

4.7.4 Benachrichtigung des Antragstellers

Vgl. Punkt 4.3.2

4.7.5 Annahme der Schlüsselerneuerung durch den Antragsteller

Vgl. Punkt 4.4.1

4.7.6 Zertifikatsveröffentlichung

Vgl. Punkt 4.4.2

4.7.7 Benachrichtigung weiterer Instanzen

Vgl. Punkt 4.4.3

4.8 Zertifikatsmodifizierung

Eine Zertifikatmodifizierung ist nicht vorgesehen. Ändern sich Antragsdaten so sind ein Zertifikatswiderruf und eine Neuausstellung des Zertifikates durchzuführen.

4.9 Widerruf und Suspendierung (Sperrung auf Zeit) von Zertifikaten

4.9.1 Gründe für einen Widerruf

Ein Zertifikat muss widerrufen werden, wenn mindestens einer der folgenden Fälle eintritt:

- Der Zertifikatsnehmer verlangt von seiner Zertifizierungsstelle schriftlich den Widerruf seines Zertifikates.
- Der Zertifikatsnehmer informiert seine Zertifizierungsstelle, dass der Zertifikatsrequest nicht autorisiert war und somit ungültig ist.
- Der private Schlüssel wurde verloren oder kompromittiert.
- Der Zertifikatsnehmer benötigt das Zertifikat nicht mehr, weil
    - er aus dem Dienst ausscheidet oder
    - er nicht mehr für den IT-Prozess verantwortlich ist, oder
    - der im Zertifikat verwendete DNS-Name nicht mehr ihm gehört (an eine andere Person/Institution vergeben wurde).
- Der Zertifikatsnehmer ist nicht mehr berechtigt, ein Zertifikat zu besitzen, z.B. weil
    - er die Zertifizierungsrichtlinie nicht einhält oder
    - die Angaben im Zertifikat nicht mehr gültig sind. (z.B. Änderung des Namens bzw. DNS-Namens bei Servern) oder
    - der im Zertifikat verwendete DNS-Name eines Servers an eine andere Person vergeben wurde oder

  - das Zertifikat nicht bestimmungsgemäß verwendet wurde, z.B. weil ein Wildcard-Zertifikat in betrügerischer Absicht benutzt wurde oder wird.

- Die Registrierungsstelle oder die Zertifizierungsstelle halten die Zertifizierungsrichtlinie oder die Regelungen zum Betrieb der Zertifizierungsstelle nicht ein.
- Die Registrierungsstelle oder Zertifizierungsstelle fällt ersatzlos weg.
- Kompromittierung des privaten CA-Schlüssels.
- Der technische Inhalt oder das Format des Zertifikates stellt ein nicht akzeptierbares Risiko für die Anbieter von Anwendersoftware oder PKI-Teilnehmer dar (z.B. ein nicht mehr empfohlener kryptographischer Signaturalgorithmus oder Schlüsselgröße).

4.9.2 Wer kann einen Widerrufsantrag stellen

Einen Widerrufsantrag darf stellen:

- der Zertifikatsnehmer bzw. ein Zertifikatsverantwortlicher bei Funktionsstellenzertifikate und Zertifikaten für IT-Prozesse,
- der rechtliche Vertreter des Zertifikatsnehmers,
- die Registrierungsstelle,
- die Wurzelregistrierungsstelle,
- die Zertifizierungsstelle,
- die Wurzelregistrierungsstelle.

4.9.3 Ablauf

Widerrufe werden nur von der Zertifizierungsstelle durchgeführt, die das zu widerrufende Zertifikat ausgestellt hat.

Der Zertifikatsnehmer muss einen Widerrufsantrag bei der Zertifizierungsstelle stellen. Hierfür hat er drei Möglichkeiten:

- über die Schnittstelle (i.d.R. durchgehend (24x7) erreichbar, Ausnahmen entsprechend SLA),
- telefonisch beim ServiceDesk des IT-DLZ im LDBV (Telefon: 089/2119-4924, entsprechend dem Servicekatalog Montag bis Freitag von 8:00 Uhr bis 16:00 Uhr erreichbar),
- persönlich bei der Registrierungsstelle.

Um einen Widerrufsantrag über die Schnittstelle zu stellen, muss sich der Zertifikatsnehmer an dieser mit seinen persönlichen Daten anmelden. Für die Durchführung des Widerrufes muss der Zertifikatsnehmer sein Sperrpasswort angeben. Die Sperrung erfolgt automatisch ohne weitere personelle Interaktion.

Für einen telefonischen Widerrufsantrag muss der Zertifikatsnehmer sein Sperrpasswort kennen und ausschnittweise dem Mitarbeiter an der Trustcenter-Hotline mitteilen. Der Mitarbeiter der Trustcenter-Hotline erfasst den Widerruf elektronisch und gibt ihn über die Web-Schnittstelle an die Zertifizierungsstelle weiter, welche den Widerruf automatisch ohne weitere personelle Interaktion durchführt.

Für einen persönlichen Widerrufsantrag wendet sich der Zertifikatsnehmer an seine Registrierungsstelle. Diese prüft dann die Identität des Antragstellers und gibt den Widerrufsantrag sofort an die Zertifizierungsstelle weiter. Hierfür wird kein Sperrpasswort benötigt. Der Mitarbeiter der Registrierungsstelle erfasst den Widerruf elektronisch und gibt ihn über die Web-Schnittstelle an die Zertifizierungsstelle weiter, welche den Widerruf automatisch ohne weitere personelle Interaktion durchführt.

4.9.4 Fristen für den Zertifikatsverantwortlichen

Bei Bekannt werden eines Widerrufgrundes muss der Zertifikatsverantwortliche unverzüglich einen Widerruf beantragen.

4.9.5 Fristen für die Zertifizierungsstelle

Die Zertifizierungsstelle muss den Widerruf innerhalb von 24 Stunden durchführen.

4.9.6 Anforderungen zu Sperrprüfungen durch den Zertifikatsprüfer

Ein Zertifikatsprüfer muss bei jedem Einsatz die Gültigkeit der Zertifikate überprüfen. Hierzu muss er die aktuelle Sperrliste beziehen und diese auf das verwendete Zertifikat prüfen.

4.9.7 Häufigkeit der Sperrlistenveröffentlichung

Die Sperrlisten der Zertifizierungsstellen sollen eine Gültigkeitsdauer von 24 Stunden besitzen und werden alle 12 Stunden neu erstellt und veröffentlicht.

4.9.8 Maximale Latenzzeit der Sperrlisten

Nach Erstellung der Sperrliste soll diese unmittelbar anschließend veröffentlicht werden.

4.9.9 Verfügbarkeit von OCSP

Die Sperrlisten der Bayern-CA sollen auch auf einem OCSP-Server veröffentlicht werden.

4.9.10 Anforderungen, um OCSP zu nutzen

Alle eingesetzten OCSP-Server werden entsprechend dem Standard RFC 2560 betrieben. OCSP-Clients sollen ebenfalls nach diesem Standard arbeiten, um ein korrekte Kommunikation zu gewährleisten.

4.9.11 Andere Formen verfügbarer Widerrufsinformationen

Außer Sperrlisten müssen keine weiteren Formen zur Verfügungstellung von Widerrufsinformationen angeboten werden.

4.9.12 Kompromittierung von privaten Schlüsseln

Bei einer Kompromittierung eines privaten Schlüssels eines Benutzers muss das zugehörige Zertifikat unverzüglich widerrufen werden.

Bei der Kompromittierung eines privaten Schlüssels einer Zertifizierungsstelle ist das Zertifikat der Zertifizierungsstelle unverzüglich zu widerrufen. Zusätzlich müssen alle von dieser Zertifizierungsstelle ausgestellten Zertifikate widerrufen werden.

4.9.13 Bedingungen, Umstände, Gründe für eine temporäre Sperrung (Suspendierung)

Eine temporäre Sperrung bzw. eine Suspendierung von Zertifikaten ist nur erlaubt, wenn es sich um Zertifikate auf Smartcards handelt.

Smartcards werden mit temporär gesperrten Zertifikaten ausgegeben, da hier eine Übergabe oder auch ein Versand zum Zertifikatsnehmer vorgesehen ist. Wenn der Zertifikatsnehmer seine Karte erhält, muss er sie über seine Registrierungsstelle endgültig aktivieren lassen. Andernfalls wird nach Ablauf einer Frist die Karte inkl. der darauf enthaltenen Zertifikate endgültig gesperrt.

4.9.14 Wer kann einen Antrag auf temporäre Sperrung stellen

Eine temporäre Sperrung wird durch die Schnittstelle der Zertifizierungsstelle gleichzeitig mit dem Zertifikatsantrag bei der Zertifizierungsstelle beantragt.

4.9.15 Verfahren zur temporären Sperrung

Im Prozess zu Erstellung einer neuen Smartcard werden die Zertifikate von der Zertifizierungsstelle nach Erstellung sofort in den Status „Temporär Gesperrt“ gesetzt.

4.9.16 Maximale Sperrdauer bei temporärer Sperrung

Zertifikate können maximal 28 Tage im Status „Temporär Gesperrt“ sein. Werden Sie in diesem Zeitraum nicht aktiviert, werden die Zertifikate danach automatisch endgültig (und dauerhaft) gesperrt.

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

4.10.1 Betriebsbedingte Eigenschaften

Der Verweis auf den OCSP-Publikationsort muss in den ausgestellten Zertifikaten hinterlegt sein.

4.10.2 Verfügbarkeit des Dienstes

Um technische Ausfälle möglichst gering zu halten, sollten OCSP-Dienste redundant aufgebaut werden.

Den OCSP-Dienst sollten alle Zertifikatsprüfer auch nutzen können D.h. weder Firewalls noch andere Zugriffsbeschränkungen sollten die Nutzung des OCSP-Dienstes durch einen Zertifikatsprüfer behindern.

4.10.3 Weitere Merkmale

Der OCSP-Dienst sollte überprüfen, ob ein angefragtes Zertifikat von der im OCSP hinterlegten Zertifizierungsstelle ausgestellt wurde. Ist dies nicht der Fall, darf der OCSP-Dienst nicht mit „good“ antworten.

4.11 Beendigung des Vertragsverhältnisses durch den Zertifikatsnehmer

Das Vertragsverhältnis kann beendet werden, wenn der Zertifikatnehmer die Dienste der Bayern-PKI nicht mehr nutzen möchte, wenn er den Arbeitgeber wechselt oder wenn die Bayern-PKI den Dienst einstellt. Wenn die Zertifikate des Zertifikatnehmers bei Beendigung des Vertragsverhältnisses noch gültig sind, müssen diese widerrufen werden.

4.12 Schlüsselhinterlegung und -wiederherstellung (Key Escrow und Recovery)

4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

Es dürfen nur Schlüssel hinterlegt werden, die der Entschlüsselung von Daten dienen. Schlüssel für Elektronische Signaturen und Schlüssel für Authentifizierung dürfen nicht hinterlegt und damit auch nicht wiederhergestellt werden.

4.12.2 Richtlinien und Praktiken zum Schutz und Wiederherstellung von Sitzungsschlüsseln

Keine Festlegung. Sitzungsschlüssel werden nicht hinterlegt.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Physikalische Sicherheitsmaßnahmen

Die für den Betrieb der Bayern-PKI notwendigen Komponenten müssen gesichert und angemessen verfügbar betrieben werden. Die Komponenten sind in physikalischen Schutzzonen unterzubringen. Der Zugang zu diesen Schutzzonen ist auf eine geschlossene Benutzergruppe zu reduzieren. Näheres ist den Regelungen zum Zertifizierungsbetrieb zu entnehmen.

5.2 Organisatorische Sicherheitsmaßnahmen

Nur berechtigtes Personal darf Funktionen im Bereich Schlüssel- und Zertifikatsmanagement ausführen oder Änderungen an der Konfiguration der CA-/RA-Software vornehmen. Diese Rechte sind in einem Rollenkonzept zu verankern.

Folgende sicherheitsrelevante Rollen sind festzulegen:

- Administratoren des PKI-Betriebs,
- Mitarbeiter der Wurzelregistrierungsstelle,
- Mitarbeiter der Registrierungsstellen,
- Auditoren.

Das LDBV als Betreiber der Bayern-PKI richtet den PKI-Betrieb und die Wurzelregistrierungsstelle ein. Die Wurzelregistrierungsstelle richtet die Zertifizierungs- und Registrierungsstellen ein. Die Wurzelregistrierungsstelle identifiziert und autorisiert die Administratoren bzw. Mitarbeiter der nachgeordneten Registrierungsstellen. Die Auditoren werden vom StMFLH benannt.

Für die Sicherheit und Verfügbarkeit der PKI werden relevante Aufgaben nach dem 4-Augen-Prinzip durchgeführt. Dazu gehören z.B. das Wiedereinspielen des Schlüsselmaterials in das kryptographische Modul sowie alle sicherheitsrelevanten Konfigurationen an der CA.

5.3 Personelle Sicherheitsmaßnahmen

Die Administratoren und die Mitarbeiter der Wurzelregistrierungsstelle und der nachgeordneten Registrierungsstellen sollen vom LDBV geschult werden, bevor sie ihre Arbeit aufnehmen. Neue Mitarbeiter einer bestehenden Registrierungsstelle sollten vom LDBV zeitnah geschult werden. Auffrischungskurse und Schulungen aufgrund größerer Änderungen sollen nach Bedarf angeboten werden.

5.4 Sicherheitsüberwachung

In den Richtlinien für den Zertifizierungsbetrieb sind zu überwachende Ereignisse so zu definieren, dass Verstöße gegen die vorliegende Zertifizierungsrichtlinie und gegen die Richtlinien für den Zertifizierungsbetrieb erkannt werden können. Die Ereignisse sind in Protokollen festzuhalten. Die Protokolle sind auszuwerten. Die Auswertung kann durch geeignete Filter- und Alarmmechanismen unterstützt werden. Die Mechanismen und die anfallenden Daten müssen regelmäßig überprüft und ausgewertet werden.

Alle Komponenten der Bayern-PKI sind durch regelmäßige Updates auf aktuellem Stand zu halten. Die Administratoren der Komponenten sind dafür verantwortlich, aktuelle Schwachstellen der Komponenten zu erkennen und diese abzustellen. Durch das Einspielen der Updates oder Patches ist mit Störungen des Betriebs zu rechnen. Es gilt das in der IT-Sicherheitsleitlinie (BayITSiLL) festgeschriebene Prinzip „Sicherheit vor Verfügbarkeit“. Die Administratoren haben ihre Aktivitäten und Prüfungen zu dokumentieren.

Bei ernst zu nehmenden Verstößen gegen die vorliegende Zertifizierungsrichtlinie und gegen die Richtlinien für den Zertifizierungsbetrieb ist der Beauftragte für IT-Sicherheit unmittelbar und unverzüglich einzuschalten.

Die Maßnahmen sind regelmäßig zu überprüfen. Die Überprüfung ist zu dokumentieren. Dabei ist in erster Linie sicherzustellen, dass die aktuellen Maßnahmen die Vorgaben erfüllen. Die Vorgaben ergeben sich aus der vorliegenden Zertifizierungsrichtlinie und den Richtlinien für den Zertifizierungsbetrieb. Die Überprüfung erfolgt durch die Auditoren.

5.5 Archivierung

Folgende Daten müssen von der Wurzelregistrierungsstelle archiviert werden:

- Alle Anträge, die eine Registrierungsstelle betreffen.

Alle Anträge zu Registrierungsstellen sind so lange zu archivieren, wie die Registrierungsstelle besteht und danach für wenigstens weitere fünf Jahre.

Folgende Daten müssen von den Registrierungsstellen archiviert werden:

- Alle Anträge, die einen Zertifikatnehmer betreffen.

Die von der Registrierungsstelle archivierten Daten sind so lange zu archivieren, wie der Zertifikatsnehmer an der Bayern-PKI teilnimmt und danach wenigstens für weitere fünf Jahre.

Folgende Daten müssen von der Zertifizierungsstelle der Bayern-PKI archiviert werden:

- Zertifikate der Zertifizierungsstellen,
- Zertifikate der Zertifikatsnehmer.

Die Zertifikate der Zertifizierungsstellen sind bis zum Ablauf der Zertifikatsgültigkeit und danach für weitere fünf Jahre zu archivieren. Die Zertifikate der Zertifikatnehmer müssen bis zum Ablauf der Zertifikatsgültigkeit und danach für weitere fünf Jahre archiviert werden.

Private Schlüssel von Zertifikatsnehmern dürfen archiviert werden.

5.6 Schlüsselwechsel der Zertifizierungsstelle

Die Gültigkeit des Zertifizierungsstellen Zertifikates muss länger sein als die Verwendungsdauer des privaten Schlüssels, d.h. der private Schlüssel der Zertifizierungsstelle darf nicht bis zum Ende der Zertifikatsgültigkeit zum Ausstellen von Zertifikaten eingesetzt werden. So wird sichergestellt, dass die nachgeordneten Zertifikate nicht länger gültig sind als das Zertifikat der ausstellenden Instanz (Schalenmodell).

Der Schlüsselwechsel der Zertifizierungsstelle muss nach dem 4-Augen-Prinzip erfolgen.

5.7 Kompromittierung einer Zertifizierungsstelle

Bei der Kompromittierung einer Zertifizierungsstelle ist der Betrieb dieser Zertifizierungsstelle unverzüglich einzustellen und das Zertifikat dieser Zertifizierungsstelle ist unverzüglich zu widerrufen. Alle von dieser Zertifizierungsstelle ausgestellten Zertifikate verlieren damit ihre Gültigkeit. Die betroffenen Benutzer sind geeignet zu informieren.

5.8 Auflösen einer Zertifizierungsstelle

Wird eine Zertifizierungsstelle aufgelöst, so muss das Zertifikat dieser Zertifizierungsstelle widerrufen werden. Das Verfahren entspricht dem Verfahren aus 5.7. Die Sperrliste muss bis zum Ende der Zertifikatsgültigkeit der Zertifizierungsstelle gültig sein.

Wird eine Registrierungsstelle aufgelöst, können die von ihr registrierten Benutzer von einer anderen Registrierungsstelle übernommen werden. Erklärt sich keine andere Registrierungsstelle zur Übernahme dieser Benutzer bereit, so müssen die Benutzer abgemeldet werden. Die zugehörigen Zertifikate werden automatisiert gesperrt.

Das Nähere regeln die Richtlinien für den Zertifizierungsbetrieb [1].

6 Technische Sicherheitsmaßnahmen

6.1 Schlüsselerzeugung und Installation

6.1.1 Schlüsselerzeugung

Die Schlüsselpaare der Zertifizierungsstellen sollen in einem kryptographischen Modul erstellt werden (vgl. 6.2).

Die Schlüsselpaare der Zertifikatsnehmer können zentral bei der Zertifizierungsstelle oder dezentral auf dem PC des Zertifikatsnehmers erstellt werden.

Die Schlüsselpaare dürfen als Datei (in Software) oder in Hardwaretoken (Chipkarte oder USB-Token) gespeichert werden.

Private Schlüssel für IT-Prozesse mit Wildcard-FQDN's, d.h. mit Stern im ersten Teil des URI's, müssen in Hardware (z.B. HSM oder Smartcard) erzeugt werden und dürfen die Hardware nicht verlassen (Ausnahme zu Backup-Zwecken).

6.1.2 Übermittlung des privaten Schlüssels an den Zertifikatsnehmer

Werden die privaten Schlüssel eines Zertifikatsnehmers zentral erstellt, muss die Übertragung des privaten Schlüssels an den Zertifikatsnehmer besonders gesichert werden, beispielsweise durch eine Transport-PIN oder ein Passwort. Private Schlüssel und Transport-PIN müssen dem Zertifikatsnehmer auf getrenntem Wege zugestellt werden.

Werden die privaten Schlüssel dezentral von den Zertifikatsinhabern selbst erzeugt, ist keine Übergabe von privaten Schlüsseln erforderlich.

6.1.3 Übermittlung des öffentlichen Schlüssels an Zertifikatsaussteller

Bei dezentraler Schlüsselerzeugung schickt der Antragsteller mit seinem Zertifikatsantrag auch seinen öffentlichen Schlüssel an die Zertifizierungsstelle. Bei der Übermittlung muss der öffentliche Schlüssel vor Veränderung gesichert werden. Nach der Zertifizierung des Schlüssels veröffentlicht die Zertifizierungsstelle den öffentlichen Schlüssel entsprechend den Veröffentlichungsrichtlinien.

6.1.4 Übermittlung des öffentlichen CA-Schlüssels an Zertifikatsprüfer

Mit Auslieferung der Zertifikate an den Zertifikatsnehmer wird ebenfalls die Zertifikatskette mitgeschickt.

Das Zertifikat der Zertifizierungsstelle der Bayern-PKI wird in den Verzeichnisdienst eingestellt und steht danach allen Kommunikationspartnern zur Verfügung.

6.1.5 Schlüssellängen

Es sollten nur Kombinationen aus Schlüsselalgorithmus und -länge verwendet werden, die als sicher gelten, d.h. es ist kein möglicher Angriff bekannt. Die eingesetzten Schlüsselalgorithmen müssen regelmäßig auf ihre Verwendbarkeit geprüft werden. Wird ein Schlüsselalgorithmus nicht mehr als sicher genug eingestuft, so dürfen keine weiteren Schlüssel ausgestellt werden, die diesen Algorithmus verwenden.

Das RSA-Schlüsselpaar der Zertifizierungsstelle der Bayern-PKI hat eine Schlüssellänge von 4096 Bits.

Für Zertifikatsnehmer müssen ebenfalls RSA-Schlüssel mit einer Länge von mindestens 2048 Bits generiert werden.

6.1.6 Parameter der öffentlichen Schlüssel und Qualitätssicherung

Die Qualität der erzeugten Public Key Parameter der Zertifizierungsstelle der Bayern-PKI sollten den vom BSI als geeignet eingestufte Kryptoalgorithmen [2] entsprechen. In beson-

deren Fällen, können die Empfehlungen des BSI als nicht bindend für die Bayern-PKI betrachtet werden. Dazu gehören beispielsweise Kompatibiltätsprobleme bei PC-Arbeitsplätzen, die dem Standard nach BayITS-11 [3] entsprechen und daher weit verbreitet sind.

6.1.7 Schlüsselverwendungszwecke und Beschränkungen

Das Zertifikat der ausstellenden Zertifizierungsstelle der Bayern-PKI enthält eine als kritisch markierte Schlüsselverwendungserweiterung (X.509v3 keyUsage extension) mit den Einträgen keyCertSign und crlSign, d.h. diese Zertifikate können nur zur Verifikation von Zertifikaten und Sperrlisten verwendet werden.

Die ebenfalls als kritisch markierte Schlüsselverwendungserweiterung (X.509v3 keyUsage extension) in den Zertifikaten für Zertifikatsnehmer dürfen folgende Einträge enthalten: DigitalSignature, nonRepudiation, keyEncipherment, dataEncipherment. Somit können sie nur für elektronische Signaturen, Authentisierung und Verschlüsselung eingesetzt werden.

6.2 Schutz des Privaten Schlüssels und Einsatz von Kryptographischen Modulen

Das Schlüsselpaar der Wurzelzertifizierungsstelle wird in einem kryptographischen Modul erstellt.

Die Schlüssel der nachgeordneten Zertifizierungsstellen der Bayern-PKI müssen ebenfalls in einem kryptographischen Modul erstellt und gespeichert werden.

Schlüssel von Zertifikatsnehmern müssen nicht in Hardware erstellt und gespeichert werden. Schlüssel mit Wildcard-FQDN‘s müssen in Hardware (z.B. HSM oder Smartcard) erzeugt werden und dürfen die Hardware nicht verlassen (Ausnahme zu Backup-Zwecken).

6.2.1 Standards des kryptographischen Moduls

Das eingesetzte kryptographische Modul muss eine Sicherheitszertifizierung nach FIPS 140 mit Level 2 oder höher besitzen.

6.2.2 Teilung des privaten Schlüssels

Die privaten Schlüssel der Zertifizierungsstelle der Bayern-PKI müssen mittels Vier-Augen-Prinzip geschützt werden.

6.2.3 Hinterlegung des privaten Schlüssels

Die privaten Schlüssel der Zertifizierungsstelle der Bayern-PKI dürfen nicht hinterlegt werden.

Die Hinterlegung privater Endanwenderschlüssel erfolgt wie in Abschnitt 4.12 angegeben.

6.2.4 Backup des privaten Schlüssels

Die privaten Schlüssel der Zertifizierungsstelle der Bayern-PKI befinden sich im HSM und müssen mit Sicherungsmethoden des HSM-Herstellers gesichert werden.

Ein Backup privater Endanwenderschlüssel erfolgt nur bei Verschlüsselungsschlüsseln, die zentral auf der Zertifizierungsstelle der Bayern-PKI erzeugt werden.

6.2.5 Archivierung des privaten Schlüssels

Es besteht keine Notwendigkeit den privaten Schlüssel der Zertifizierungsstelle der Bayern-PKI nach Ende seiner Nutzung noch länger aufzubewahren.

6.2.6 Transfer des privaten Schlüssels in oder aus einem kryptographischen Modul

Abgesehen von der Sicherung und ggf. einer Wiederherstellung mit Sicherungsmethoden des HSM-Herstellers findet kein Transfer des privaten Schlüssels statt.

6.2.7 Speicherung des privaten Schlüssels in einem kryptographischen Modul

Der private Schlüssel der Zertifizierungsstelle der Bayern-PKI wird verschlüsselt im HSM abgelegt.

6.2.8 Aktivierung des privaten Schlüssels

Zum Aktivieren des privaten Schlüssels der CA für die Zertifizierung von Endanwenderschlüsseln genügt die Eingabe eines Passwortes beim Start des Zertifizierungsdienstes auf dem CA-Server. Ebenfalls per Passworteingabe bei Dienststart wird die Signatur der Sperrlisten aktiviert.

Private Schlüssel von Endanwendern müssen mindestens mit einem Passwort/ PIN gesichert sein, welches beim Aktivieren des privaten Schlüssels eingegeben werden muss. Zusätzlich dürfen private Schlüssel von Endanwendern durch eine Speicherung der privaten Schlüssel auf einem Hardwaretoken (Smartcard oder USB-Token) gesichert werden.

6.2.9 Deaktivierung des privaten Schlüssels

Der private Schlüssel der Zertifizierungsstelle der Bayern-PKI wird deaktiviert, sobald der Zertifizierungsdienst auf dem CA-Server gestoppt wird.

Zur Deaktivierung privater Schlüssel von Endanwendern sind folgende Möglichkeiten erlaubt:

1. Bleibt der private Schlüssel nach Aktivierung einige Zeit ungenutzt, wird er automatisch deaktiviert.
2. Die Software zur Zertifikatsverwaltung bietet die Möglichkeit, Schlüssel manuell wieder zu deaktivieren, beispielsweise über eine Schaltfläche.
3. Sind die privaten Schlüssel auf einem Hardwaretoken gespeichert, erfolgt die Deaktivierung beim Entfernen des Tokens aus dem Lesegerät.
4. Eine Aktivierung des privaten Schlüssels soll immer nur für eine Aktion gültig bleiben und danach soll der Schlüssel automatisch wieder deaktiviert werden.

6.2.10 Vernichtung des privaten Schlüssels

Die Vernichtung eines privaten Schlüssels einer CA kann aus zwei Situationen heraus in Frage kommen:

- der Nutzungszeitraum des CA-Schlüssels ist abgelaufen oder
- der Schlüssel der CA wurde widerrufen/ gesperrt.

6.2.11 Güte des Kryptographischen Moduls

Das kryptographische Modul verfügt über eine Sicherheitszertifizierung nach FIPS 140-2 Level 3.

6.3 Andere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel, die von der Zertifizierungsstelle der Bayern-PKI zertifiziert wurden, werden in der Datenbank der Zertifizierungsstelle archiviert

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Zertifikate und Schlüssel für die Wurzelzertifizierungsstelle dürfen max. 15 Jahre gültig sein.

Zertifikate und Schlüssel für Zertifizierungsstellen dürfen max. 8 Jahre gültig sein.

Zertifikate und Schlüssel für Zertifikatsnehmer (Personen bzw. Funktionsstellen) dürfen nicht länger als 3 Jahre gültig sein. Zertifikate und Schlüssel für automatisierte IT-Prozesse dürfen 1 Jahr gültig sein.

Die Gültigkeit des CA-Zertifikates muss länger sein als die Verwendungsdauer des privaten Schlüssels, d.h. der private Schlüssel der CA darf nicht bis zum Ende der Zertifikatsgültigkeit zum Ausstellen von Zertifikaten eingesetzt werden. So wird sichergestellt, dass die nachgeordneten Zertifikate nicht länger gültig sind als das Zertifikat der ausstellenden Instanz (Schalenmodell).

6.4 Aktivierungsdaten

Werden die privaten Schlüssel eines Zertifikatsnehmers zentral erstellt, muss die Übertragung des privaten Schlüssels an den Zertifikatsnehmer besonders gesichert werden. Dafür kann der private Schlüssel für den Übertragungsweg mit einem Transport-PIN versehen werden. Dieser Transport-PIN muss dem Zertifikatsnehmer auf einem anderen Wege mitgeteilt werden, als er den privaten Schlüssel erhalten hat.

Die Speicherung des privaten Schlüssels auf dem PC/ System des Zertifikatsnehmers soll immer gesichert, also z.B. mit Passwortschutz erfolgen. Sobald der private Schlüssel verwendet wird, muss der Zertifikatsnehmer diesen Schutz zunächst lösen.

6.4.1 Erstellung und Installation der Aktivierungsdaten

Bei zentraler Schlüsselerstellung müssen die Aktivierungsdaten (PIN, Passwort), die den privaten Schlüssel schützen, durch eine gesicherte Applikation erstellt und besonders gesichert an den Anwender übertragen werden.

Sobald der Anwender Schlüssel und Aktivierungsdaten erhalten hat, muss er die Aktivierungsdaten (PIN, Passwort) ändern.

Für die geänderten Aktivierungsdaten sind mindestens 6 Zeichen aus wenigstens 2 Zeichengruppen (Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen) zu verwenden.

6.4.2 Schutz der Aktivierungsdaten

Die Aktivierungsdaten sind geeignet vor Verlust, Diebstahl, Veränderung, nicht autorisiertem Offenlegung oder nicht autorisierter Verwendung zu schützen.

6.4.3 Weitere Aspekte

Keine Festlegung.

6.5 Sicherheitsmaßnahmen für Computer

6.5.1 Spezifische Anforderungen an die technischen Sicherheitsmaßnahmen

Es wird auf die Anforderungen der Richtlinie BayITS-11 [3] verwiesen, die Sicherheitsmaßnahmen für alle Standardarbeitsplätze in der Staatsverwaltung regelt.

Server der zentralen Infrastruktur sind nach BSI-Grundschutz zertifiziert.

Andere Server sollen ebenfalls die Vorgaben des BSI-Grundschutzes erfüllen. Dazu gehören z.B.

- Penetrationstest,

- Minimalsystem – nur benötigte Software ist installiert,
- bei sicherheitskritischen Fehlern muss das System schnellstmöglich auf einen aktuellen Sicherheitsstand gebracht werden; evtl. ist eine vorübergehende Betriebsruhe in Betracht zu ziehen,
- sicherheitsrelevante Vorgänge sind zu protokollieren,
- eingeschränkte Zugangs- und Zugriffsberechtigungen,
- eingeschränkte Kommunikationsschnittstellen – nur benötigte Kommunikationsschnittstellen.

6.5.2 Güte der Sicherheitsmaßnahmen

Für Komponenten der zentralen Infrastruktur muss eine Bedrohungsanalyse durchgeführt und ein geeignetes Sicherheitskonzept erstellt werden.

6.6 Technische Sicherheitsmaßnahmen des Software-Lebenszyklus

Für Software im Bereich der Benutzer- und Zertifikatsverwaltung sollen weitestgehend Standardprodukte verwendet werden, die möglichst geringe Anpassungen an die Betriebsumgebung benötigen.

6.6.1 Maßnahmen der Systementwicklung

Die verwendete Software muss allgemein bekannten Bedrohungsszenarien standhalten.

PKI-Systeme sind so zu entwickeln, dass der Hersteller keinen vom Betreiber unbemerkten Zugriff auf die Betriebsdaten (private Schlüssel, PINs, Benutzerdaten) hat.

6.6.2 Maßnahmen im Sicherheitsmanagement

Die Systemadministration muss auf den erhöhten Sicherheitsbedarf der PKI-Komponenten hingewiesen werden. Insbesondere ist organisatorisch zu regeln, dass die Betriebsdaten (private Schlüssel, PINs, Benutzerdaten) nicht durch die Systemadministration gelesen oder weitergegeben werden dürfen.

Es ist weiterhin (organisatorisch) zu regeln, dass die Entwickler der Systeme/ Software keinen Zugang zu den Betriebsdaten der Betriebsumgebung haben. Wenn Entwickler, z.B. bei der Behebung von Fehlern, in der Betriebsumgebung arbeiten müssen, so ist von Seiten der Entwickler Vertraulichkeit einzufordern.

Müssen den Entwicklern Protokolle der Systeme übergeben werden (z.B. zur Fehlersuche), so sind nicht benötigte Daten, insbesondere Betriebsdaten, zu entfernen.

Software-Aktualisierungen und -Erweiterungen sind vom Hersteller gesichert vor Veränderungen an den Betreiber des Systems zu übermitteln (Integrität). Betriebssystemaktualisierungen und neue Programmversionen müssen vor dem Einspielen in die Betriebsumgebung funktionalen und qualitätssichernden Tests unterzogen werden.

Vor Inbetriebnahme der PKI-Komponenten sollen Penetrationstests der Betriebsumgebung durchgeführt werden. Diese und vergleichbare Tests sollen in regelmäßigen Abständen wiederholt werden.

6.6.3 Lebenszyklus der Sicherheitsmaßnahmen

Keine Festlegung.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Für eine erhöhte Sicherheit der PKI sind Komponenten, die private Schlüssel erstellen, verarbeiten oder speichern, mit entsprechenden Sicherheitsmaßnahmen zu versehen, dazu gehört auch die Netzwerksicherheit.

Die umgesetzten Sicherheitsmaßnahmen im Netzwerk werden in den Regelungen zum Zertifizierungsbetrieb [1] beschrieben.

6.8 Zeitstempel

Ein Zeitstempeldienst wird derzeit nicht angeboten.

7 Profile für Zertifikate, Widerrufslisten und Online-Statusabfragen

7.1 Zertifikatsprofile

Die ausgestellten Zertifikate entsprechen X.509v3.

Ein Zertifikatsnehmer darf pro Zertifikatstyp nur ein gültiges Zertifikat besitzen.

7.2 Widerrufslistenprofile

Die ausgestellten Sperrlisten entsprechen CRLv2.

7.3 OCSP Profile

OCSP-Antworten entsprechen dem Standard nach RFC 2560.

8 Konformitätsprüfung

Die Arbeitsprozesse der Zertifizierungs- und Registrierungsstellen müssen regelmäßig auf Konformität mit der Zertifizierungsrichtlinie und den Regelungen für den Zertifizierungsbetrieb überprüft werden.

8.1 Frequenz und Umstände der Überprüfung

Die erste Überprüfung soll vor Aufnahme des Betriebs einer Zertifizierungs- oder Registrierungsstelle erfolgen. Weitere Überprüfungen einer Zertifizierungs- und Registrierungsstelle sollen regelmäßig vorgenommen werden. Registrierungsstellen sollen mindestens einmal pro Jahr überprüft werden.

8.2 Identität des Überprüfers

Die Überprüfung der Wurzelregistrierungsstelle und der Zertifizierungsstellen muss durch das StMFLH oder durch eine vom StMFLH beauftragte Stelle erfolgen.

8.3 Verhältnis von Prüfer zu Überprüftem

Der Prüfer darf nicht gleichzeitig ein Mitglied der zu überprüfenden Stelle sein. Eine Selbstüberprüfung ist nicht gestattet. Unter einer Stelle wird in diesem Zusammenhang eine Behörde, eine Abteilung oder ein Sachgebiet verstanden.

8.4 Überprüfte Bereiche

Es können alle für die PKI relevanten Bereiche überprüft werden.

8.5 Mängelbeseitigung

Festgestellte Mängel müssen zeitnah, in Absprache zwischen Prüfer und Geprüftem, beseitigt werden. Kommt eine Registrierungsstelle der Mängelbeseitigung während des vereinbarten Zeitraums nicht nach, muss der Prüfer eine Stilllegung der Registrierungsstelle bei der Wurzelregistrierungsstelle veranlassen. Kommt eine Zertifizierungsstelle der Mängelbeseitigung während des vereinbarten Zeitraums nicht nach, so muss der Prüfer eine Sperrung des Zertifikats der übergeordneten Zertifizierungsstelle veranlassen.

8.6 Veröffentlichung der Ergebnisse

Eine Veröffentlichung der Ergebnisse außerhalb der betroffenen Stellen ist nicht vorgesehen.

9 Rechtliche Vorschriften

9.1 Gebühren

Derzeit werden keine Gebühren erhoben.

9.2 Finanzielle Verantwortung

Eine Insolvenz des LDBV kann nicht eintreten, so dass eine Abdeckung der finanziellen Verantwortungen des LDBV durch Versicherungen nicht erforderlich ist.

9.3 Vertraulichkeit von Informationen

Alle Informationen, die nicht vom LDBV veröffentlicht werden, werden vertraulich behandelt.

9.4 Datenschutz

Das LDBV und die Registrierungsstellen beachten alle gesetzlichen Bestimmungen über den Datenschutz.

Daten werden im Rahmen der Diensterbringung an Dritte nur im Rahmen vertraglicher Regelungen weitergegeben, wenn eine unterzeichnete Vertraulichkeitserklärung des Dritten vorliegt, in der dieser die mit der Aufgabe betrauten Mitarbeiter zur Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet hat.

9.5 Urheberrechte

Es gelten die gesetzlichen Bestimmungen. In dieser Zertifizierungsrichtlinie werden keine besonderen Regelungen getroffen.

9.6 Gewährleistung

Siehe Abschnitt 9.7

9.7 Gewährleistungsausschluss

Das LDBV und die Registrierungsstellen übernehmen trotz Einhaltung aller erforderlichen Sicherheitsmaßnahmen keine Gewähr dafür, dass die für die Zertifizierung benötigten Datenverarbeitungssysteme ohne Unterbrechung betriebsbereit sind und fehlerfrei arbeiten. Datenverluste infolge technischer Störungen und die Kenntnisnahme vertraulicher Daten durch unberechtigte Eingriffe sind auch bei Beachtung der erforderlichen Sorgfalt nie völlig auszuschließen.

9.8 Haftungsbeschränkung

Im Haftungsfall ist die Haftung für jedes haftungsauslösende Ereignis betragsmäßig auf 0,00 € beschränkt.

9.9 Haftungsfreistellung

Siehe Abschnitt 9.8

9.10 Inkrafttreten und Aufhebung der Zertifizierungsrichtlinie

Diese Zertifizierungsrichtlinie tritt am Tag ihrer Veröffentlichung in Kraft. Die Gültigkeit der Zertifizierungsrichtlinie endet bei Veröffentlichung einer neuen Zertifizierungsrichtlinie oder mit Einstellung der Zertifizierungsdienste der Wurzelzertifizierungsstelle (BSI) oder des LDBV.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

In dieser Zertifizierungsrichtlinie werden keine entsprechenden Regelungen getroffen.

9.12 Änderungen/Ergänzungen der Richtlinien

Neue Versionen der Zertifizierungsrichtlinie werden auf der Web-Seite des LDBV veröffentlicht. Teilnehmende Zertifizierungsstellen werden über neue Versionen unterrichtet.

Das LDBV entscheidet, ob bei Änderungen der Zertifizierungsrichtlinie ein neuer Policy-Identifier verwendet wird. Dies wird insbesondere dann der Fall sein, wenn die Zertifizierungsrichtlinie erhebliche Änderungen gegenüber der vorangegangenen Zertifizierungsrichtlinie aufweist.

9.13 Schiedsverfahren

Zur Beilegung telekommunikationsrechtlicher Streitigkeiten kann die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen einen einvernehmlichen Einigungsversuch vor einer Gütestelle gemäß § 124 TKG vorschlagen.

9.14 Gerichtsstand

Für Streitigkeiten aus dieser Zertifizierungsrichtlinie gilt die ausschließliche Zuständigkeit des Landgerichts München I.

9.15 anwendbares Recht

Es gilt deutsches Recht.

9.16 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.

10 Glossar

AIA	Authority Information Access, Angabe im Zertifikat zum Veröffentlichungspunkt des übergeordneten CA-Zertifikates
Automatisierter IT-Prozess	kann z.B. Zertifizierungsstelle, Serverprozesse mit Signatur, SSL-Server, Workstations, Mobile Device Management Systeme sein
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYBN	Bayerisches Behördennetz
CA	Certification Authority, Zertifizierungsinstanz
CA-Policy	Zertifizierungsrichtlinie einer PKI; das vorliegende Dokument
CDP	CRL Distribution Point, Angabe im Zertifikat zum Veröffentlichungspunkt der Sperrliste
CPS	Certificate Practice Statement, Regelungen für den Zertifizierungsbetrieb
CRL	Certificate Revocation List, Sperrliste
DN	Distinguished Name, siehe DName
DName	Distinguished Name, ein eindeutiger Objektname in LDAP-Verzeichnissen
Endstellen-CA	Zertifizierungsinstanz, die Zertifikate für Endstellen ausstellt (z.B. für Benutzer, Funktionsstellen oder IT-Prozesse)
Hardwaretoken	Ein Hardwaretoken ist eine Hardware zur Speicherung von privaten Schlüsseln, die u. a. eine unberechtigte Nutzung des privaten Schlüssels verhindert.
HSM	Hardware Security Module, an den CA-Server angeschlossenes Modul zur sicheren Aufbewahrung von Verschlüsselungs- und Signaturschlüsseln der CA
IT-DLZ / RZ-Süd	Rechenzentrum Süd; ein Betriebsteil des LDBV und Betreiber der bayerischen Verwaltungs-PKI
Key Backup	Sicherung von privaten Verschlüsselungsschlüsseln zur späteren Wiederherstellung
Key Recovery	Wiederherstellung von privaten Schlüsseln auf Anforderung des Besitzers, z.B. wenn der private Schlüssel verloren gegangen ist und etwas entschlüsselt werden muss
Key Escrow	Wiederherstellung von privaten Schlüsseln auf Anforderung eines Dritten, z.B. bei längerer Krankheit des Besitzers, wenn in seiner Abwesenheit etwas entschlüsselt werden muss
LDAP	Light Directory Access Protocol, Verzeichnisdienst (z.B. für Zertifikate oder Sperrlisten)
LDBV	Landesamt für Digitalisierung, Breitband und Vermessung
NIST	National Institute of Standards and Technology, US-amerikanische Bundesbehörde, die für Standardisierungsprozesse zuständig ist
OCSP	Online Certificate Status Protocol
PGP	Pretty Good Privacy

PKI	Public Key Infrastructure, organisatorische und technische Einheit, deren Teilnehmer von einer gemeinsamen Root-CA zertifiziert werden
PSE	Personal Security Environment (PSE), gesicherter Zertifikatsspeicher
PIN	Personal Identification Number, geheime Zahl- oder Zeichenfolge (z.B. um den privaten Schlüssel zu schützen)
RA	Registration Authority, Registrierungsstelle
Registrierungsstelle	Stelle, die eine Person als Teilnehmer registriert und identifiziert
RFC	Request for Comment, Dokumente für weltweite Standardisierungen
RFC3647	Dieses RFC dient der Beschreibung von Dokumenten, die den Betrieb einer PKI beschreiben, insbesondere der CA-Policy und des CPS.
RFC2560	Dieses RFC dient der Beschreibung von OCSP.
RFC6960	Dieses RFC dient der Beschreibung von OCSP. Er ersetzt den älteren RFC 2560.
RFC-822 Name	E-Mail Adresse
Root-CA	vgl. Wurzel-CA
Schlüsselpaar	Ein Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüssel. Der private Schlüssel ist nur dem Besitzer zugänglich und bedarf eines besonderen Schutzes. Der öffentliche Schlüssel ist allen Teilnehmern bekannt.
SigG	Signaturgesetz; gibt Rahmenbedingungen vor, unter denen eine digitale Signatur einer handschriftlichen rechtlich gleichgestellt ist.
S/MIME	Secure Multipurpose Internet Mail Extensions, Standard für Sichere E-Mail
Sperrliste	Liste, die von einer CA ausgestellt und signiert wird und gesperrte Zertifikate enthält
SSL	Secure Socket Layer, Protokoll zur Transportsicherung einer Client-Server-Kommunikation
StMFLH	Staatsministerium der Finanzen, dem LDBV übergeordnete Dienststelle und Auftraggeber der Bayerischen Verwaltungs-PKI
Trustcenter	Zertifizierungsdiensteanbieter
UID	Unique Identifier, eindeutige Zahl
URI	Uniform Resource Identifier, eine Zeichenfolge, die zur Identifizierung einer Ressource dient (z.B. zur Bezeichnung von Ressourcen im Internet und dort vor allem im WWW)
Widerrufsliste	(siehe Sperrliste)
Wurzel-CA	oberste Zertifizierungsinstanz in einer PKI
X.509v3	Zertifikatsstandard

Zertifikat	sichert die Zuordnung von öffentlichem Schlüssel zu einem Teilnehmer
Zertifizierungsinstanz	Stellt Zertifikate aus.

11 Referenzen

[1] Richtlinien für den Zertifizierungsbetrieb

[2] BSI, Technische Richtlinie (BSI TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen)
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

[3] BayITS-11, IT-Standards für die bayerische Staatsverwaltung - PC-Arbeitsplatz
http://www.cio.bybn.de/intranet/cio/4/19809/index.htm?ref=/intranet/cio/4/19819/index.htm (ausschließlich im Behörden-Intranet)