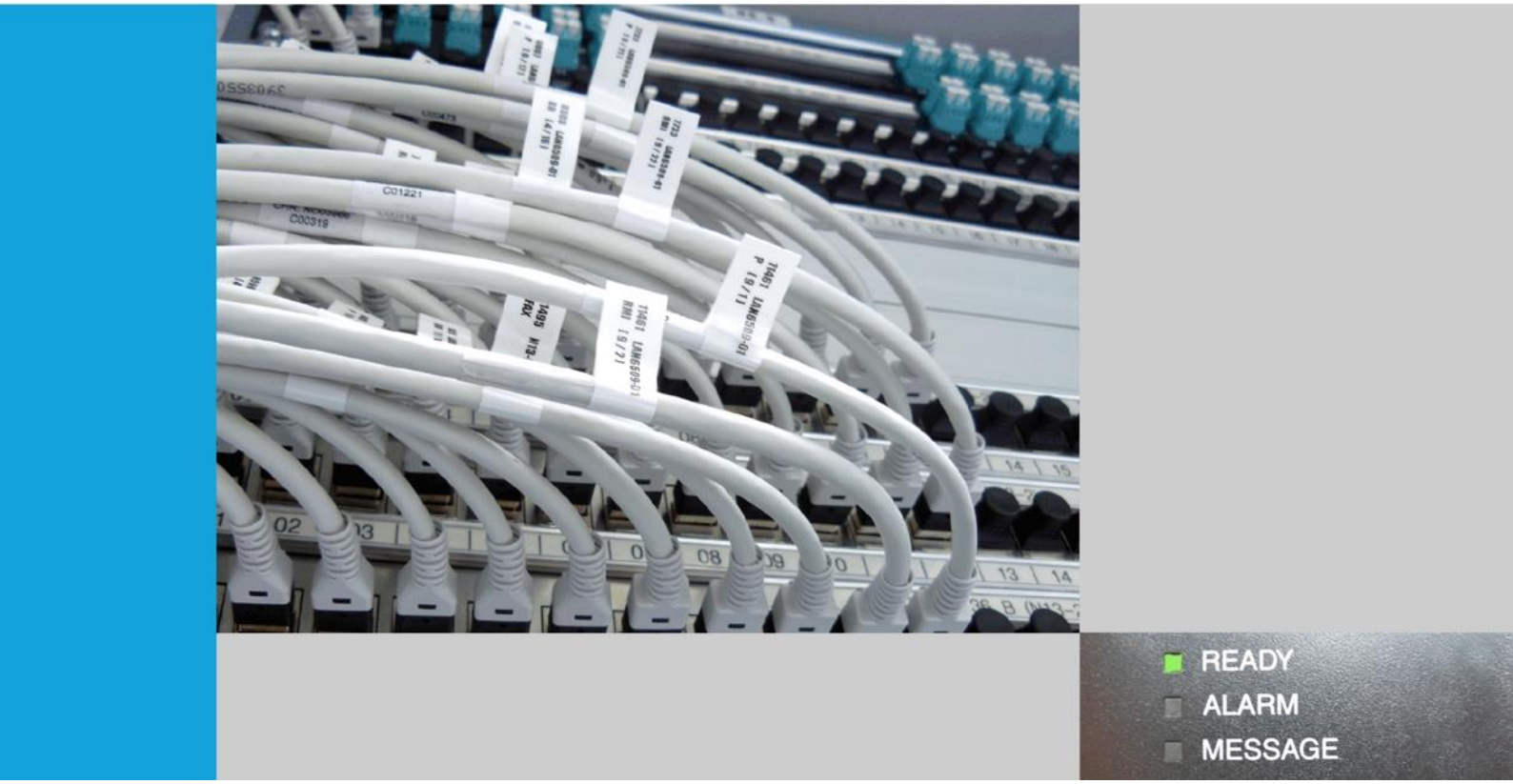
Landesamt für Digitalisierung,
Breitband und Vermessung

IT-Dienstleistungszentrum des Freistaats Bayern



Zertifizierungsrichtlinie (CP) und Regelungen zum Zertifizierungsbetrieb (CPS) der Public Key Infrastructure der Bayerischen Verwaltung

für die
X.509-Zertifizierungshierarchie der
Bayerischen SSL-Server-PKI

Bearbeitung:
Kerstin Ehrhardt

München, den 12.4.2019

Dokumentenentwicklung

Version	Datum	Bearbeiter	Beschreibung, QS-Maßnahme	Status *s. u.
1.0	08.01.2013	K. Ehrhardt	Version 1.0 veröffentlicht	freigegeben
1.2	09.02.2018	K. Ehrhardt	Neue Designvorlage; inhaltlicher Review	freigegeben
1.3	12.04.2019	K. Ehrhardt	Inhaltlicher Review; Änderungen in folgenden Abschnitten: 3.3.1, 4.1.2, 4.3.1, 4.4.1, 4.7.2, 4.7.3, 6.1.1, 6,1,2, 6.1.5, 6.4, 6.4.1	freigegeben

* zu verwenden sind: in Bearbeitung, vorgelegt, freigegeben

Inhaltsverzeichnis

1 Einführung

Das IT-Dienstleistungszentrum im Bayerischen Landesamt für Digitalisierung, Breitband und Vermessung (LDBV) betreibt im Auftrag des Bayerischen Staatsministeriums der Finanzen, für Landesentwicklung und Heimat (StMFLH) 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, deren Wurzel (Root) von QuoVadis (http://www.quovadisglobal.com/) betrieben wird. Gemäß den Richtlinien der QuoVadis Root-CA wird in dieser PKI ausschließlich die Ausstellung von Zertifikaten für SSL-Server angeboten (im Folgenden SSL-Server-Zertifikate genannt).

- Die Firma QuoVadis betreibt die Wurzel-CA. Diese CA zertifiziert nachgeordnete Sub-CA's u.a. eine der Bayerischen Verwaltung.
- Die Wurzel-CA ist in den meisten Webbrowsern und Betriebssystemen als „Vertrauenswürdige Stammzertifizierungsstelle" eingetragen.
- Das LDBV betreibt eine Sub-CA im Bayerischen Behördennetz.

1.1 Überblick

1.1.1 Aufbau und Zweck des Dokumentes

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

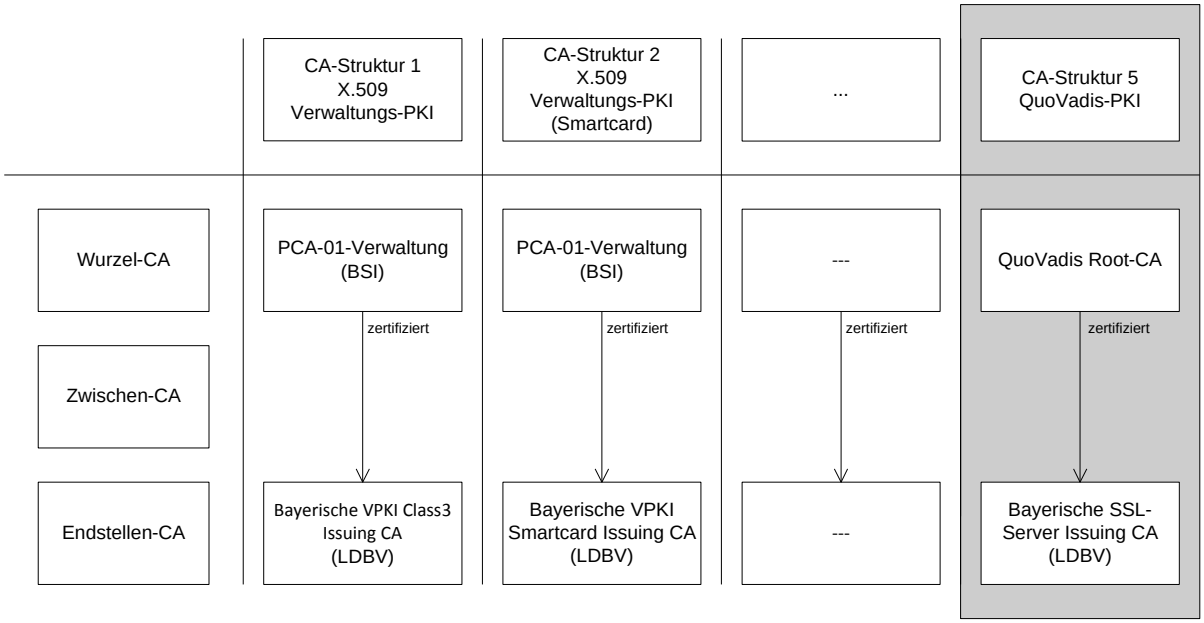
Die technischen Maßnahmen und Prozesse sind detailliert im Betriebshandbuch [1] beschrieben. Die Zertifizierungsrichtlinie orientiert sich an den Vorgaben aus RFC 3647. Des Weiteren müssen Anforderungen und Richtlinien des CA/Browser-Forums berücksichtigt werden. Dazu gehören u.a. die Baseline Requirements [3].

Diese Zertifizierungsrichtlinie muss der Firma QuoVadis als zertifizierende Instanz vorgelegt werden. Inhaltliche Änderungen müssen mit der Firma QuoVadis abgestimmt werden.

1.1.2 Aufbau der Bayerischen Verwaltungs-PKI

Die Bayerische Verwaltungs-PKI 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 X.509-Zertifizierungshierarchie, die ausschließlich SSL-Server-Zertifikate in der staatlichen und kommunalen Verwaltung Bayerns zur Verfügung stellt. Sie ist nicht Teil der Deutschen Verwaltungs-PKI, die vom BSI betrieben wird.



1.2 Name und Identifikation des Dokumentes

Name:	Zertifizierungsrichtlinie der Bayerischen SSL-PKI
Version:	1.3
Datum:	12.04.2019
Object Identifier (OID):	1.3.6.1.4.1.19266.1.2.3

Die SSL-CA erfüllt die Anforderungen der aktuellen Version der „Baseline Requirements for the Issuance an Management of Publicly-Trusted Certificates“[3]. Im Falle von Inkonsistenzen zwischen der vorliegenden Policy und den vorgenannten „Baseline Requirements“ haben die „Baseline Requirements“ Vorrang.

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen

Die Zertifizierungsstellen geben Zertifikate für Zertifikatsnehmer aus. Für die SSL-PKI ist eine maximal dreistufige PKI-Hierarchie vorgegeben. In dieser Hierarchie bilden die Zertifikatsnehmer die unterste Stufe und die Wurzelzertifizierungsstelle die oberste Stufe.

Die Wurzelzertifizierungsstelle zertifiziert ausschließlich nachgeordnete Zertifizierungsstellen. Die nachgeordneten Zertifizierungsstellen stellen ausschließlich Endstellenzertifikate aus.

Die Wurzelzertifizierungsstelle der SSL-PKI ist die QuoVadis Root CA 3 G3. Der Object Identifier (OID) des Root CA Zertifikates ist 1.3.6.1.4.1.8024.0.3.

1.3.2 Registrierungsstellen

Für die Bayerische SSL-PKI wird die vorhandene Struktur von Registrierungsstellen, die bereits für die Bayerische Verwaltungs-PKI aufgebaut und genutzt wird, genutzt. Es gibt 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 werden von der Wurzelregistrierungsstelle in Räumen des LDBV geschult und sind danach 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 ausschließlich für die staatliche und kommunale Verwaltung in Bayern ausgegeben.

Zertifikatsnehmer können ausschließlich automatisierte IT-Prozesse (SSL-Server) sein.

Zertifikatsverantwortliche:

Für Zertifikate oder Schlüssel muss immer eine einzelne natürliche Person verantwortlich sein (im Folgenden als Zertifikatsverantwortlicher bezeichnet). Der Zertifikatsverantwortliche muss der Registrierungsstelle einen entsprechenden Zuständigkeitsnachweis beibringen.

1.3.4 Zertifikatsprüfer

Zertifikatsprüfer überprüfen anhand eines Zertifikates der Bayerischen SSL-PKI die Authentizität eines SSL-Servers. Für die Überprüfung werden das Zertifikat selbst, 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 Verwaltung der Richtlinien

1.4.1 Änderungsmanagement

Die vorliegende Zertifizierungsrichtlinie wird durch das LDBV verwaltet. Änderungen an der Zertifizierungsrichtlinie werden im Abschnitt Änderungshistorie zu Beginn des Dokumentes protokolliert. Änderungen an der Zertifizierungsrichtlinie müssen mit dem StMFLH abgestimmt werden. Der Betreiber der Root-CA (QuoVadis) muss darüber informiert werden. Bei gravierenden Änderungen sollte der Betreiber der Root-CA (QuoVadis) einbezogen werden.

1.4.2 Ansprechstelle

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

Telefon: 089/2119-4924
Fax: 089/2119-14873
E-Mail: pki-support@ldbv.bayern.de

1.4.3 Eignungsprüfer für Regelungen zum Zertifizierungsbetrieb gemäß Zertifizierungsrichtlinie

In regelmäßigen Selbstüberprüfungen soll geprüft werden, ob die Regelungen zum Zertifizierungsbetrieb die Anforderungen der Zertifizierungsrichtlinie geeignet erfüllen.

1.4.4 Verfahren zur Anerkennung von Regelungen zum Zertifizierungsbetrieb

Die Regelungen zum Zertifizierungsbetrieb sind dem StMFLH als Auftraggeber und der Wurzel-Zertifizierungsstelle aus Verlangen vorzulegen. Die Wurzel-Zertifizierungsstelle entscheidet anschließend über den Zertifizierungsbetrieb.

1.5 Definitionen und Abkürzungen

Siehe Glossar

2 Veröffentlichungen und Verzeichnisdienst

2.1 Verzeichnisdienst

Die Zertifizierungsstellen stellen die von ihnen ausgestellten Sperrinformationen in einen Verzeichnisdienst ein, welcher vom Internet aus erreichbar ist. Der Abruf der Informationen erfolgt über LDAPv3 gemäß RFC 2251. Der Abruf der Sperrinformationen soll zusätzlich auch über OCSP möglich sein.

Die Zertifizierungsstellen- und Serverzertifikate sollen im Verzeichnisdienst in dem durch den Namen des Zertifikatsnehmers 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

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.

Die technischen Informationen, um sich auf die Verzeichnisdienste zu verbinden, werden im Internet unter http://www.pki.bayern.de veröffentlicht.

Dem Betreiber der Wurzel-CA werden zusätzlich alle ausgestellten Endstellenzertifikate zur Verfügung gestellt. Diese Informationen unterliegen besonderem Schutz und werden deshalb nicht in einem öffentlich lesbaren Verzeichnis abgelegt. Die Zugangsdaten zu diesem Verzeichnis erhält ausschließlich der Betreiber der Wurzel-CA.

Im Rahmen von Certificate Transparency werden alle ausgestellten Zertifikate in sogenannten CT Logs geführt. Diese Logs sind öffentlich bekannte Dateien im Klartext. Sie werden automatisch von Webbrowsern ausgelesen und zur Verifikation einer mit SSL gesicherten Webseite benutzt.

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 Zertifikate von Zertifizierungsstellen und Sperrinformationen muss anonym erfolgen. Der lesende Zugriff auf veröffentlichte Endstellenzertifikate ist nur für den Betreiber der Wurzel-CA bestimmt. Der schreibende Zugriff ist auf berechtigte Personen bzw. automatisierte IT-Prozesse 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.

Die Wurzel-CA hat der Bayerischen Verwaltungs-PKI einen eindeutigen Namensraum zugewiesen. Innerhalb der SSL-PKI ist dieser Namensraum zu verwenden.

3.1.1 Namenstypen

Die folgenden Namenstypen sollen unterstützt werden:

- DName
- URI
- LDAP-Namen
- Principalname
- DNS-Name

Zertifikatsinhaber und Zertifikatsaussteller müssen einen eindeutigen DName zugewiesen bekommen. Der URI im Attribut Subject soll automatisierte IT-Prozesse kennzeichnen. Die LDAP-Namen müssen auf die Einträge verweisen, wo das Zertifikat und die Sperrliste der Bayerischen Infrastruktur-PKI-CA im LDAP-Verzeichnis veröffentlicht sind. Ein Principal Name ist eine eindeutige Zeichenkette (Name) im Active Directory und bezeichnet z.B. eine Serviceinstanz (Service Principal Name, SPN). Wird ein DNS-Name verwendet, so bezeichnet er einen eindeutigen Namen im Netzwerk für eine Maschine, z.B. einen Server.

Beim Namenstyp DName sind folgende Festlegungen zu beachten:

- Im Attribut Subject/ Antragsteller eines Zertifikats für Zertifizierungsstellen müssen im DName die Bestandteile „organizationName“ (o), „stateOrProvince“ (s) und „countryName“ (c) enthalten sein.
- Im Attribut Subject/ Antragsteller eines Zertifikats für Endstellen müssen im DName die Bestandteile „commonName“ (cn), „organizationalUnitName“ (ou), „organizationName“ (o), „stateOrProvince“ (s) und „countryName“ (c) enthalten sein.

Beim Namenstyp DNS-Name sind folgende Festlegungen zu beachten:

- In den „Baseline Requirements“ des CAB Forums [3] ist festgelegt, dass keine internen Servernamen oder reservierten IP-Adressen verwendet werden dürfen. Jeder Servername muss durch einen DNS-Server im Internet auflösbar sein.

3.1.2 Aussagekraft von Namen

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

- Zertifikate für SSL-Server dürfen nicht auf die Namen von natürlichen oder juristischen Personen ausgestellt werden.
- Der Name der Serverinstanz muss eindeutig hervorgehen.
- Wildcard-Zertifikate sind unter bestimmten Voraussetzungen erlaubt (vgl. 6.1.1 und 6.2).

Die Einhaltung der Namenskonventionen ist von der zuständigen Zertifizierungsstelle sicherzustellen.

3.1.3 Anonyme und Pseudonyme

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

3.1.4 Namensinterpretation

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 Bayerische SSL-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 dieser 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 (Servern)

Registrierungsstellen müssen sich als Funktion bei der Wurzelregistrierungsstelle registrieren.

Zertifikatsnehmer müssen sich bei einer der Wurzelregistrierungsstelle nachgeordneten Registrierungsstelle authentisieren.

Sollen Zertifikate für Server 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.

Die Zertifizierungsstelle darf nur Server mit Zertifikaten ausstatten, die ihr bekannt sind. Die Zertifizierungsstelle muss die Authentifizierung eines IT-Prozesses 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 (Personal-

ausweis, 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

Es erfolgt keine Prüfung durch die Registrierungsstelle, inwieweit der benannte Zertifikatsverantwortliche tatsächlich für den beantragten Server 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.

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 der Web-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 Wurzelzertifizierungsstelle, die Wurzelregistrierungsstelle oder die Registrierungsstelle sollen 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 eine webbasierte Schnittstelle (Web-Frontend) zur Verfügung.

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

Im Zuge der erstmaligen Anmeldung an der Web-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 Web-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. Web-Schnittstelle bereit.

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

4.2 Bearbeitung von Zertifikatsanträgen

4.2.1 Durchführung von Identifikation und Authentifizierung

Vor der Antragstellung muss sich der Antragsteller bei einer Registrierungsstelle authentifizieren. Die Registrierungsstelle pflegt die Antragstellerdaten in die Web-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).

4.2.2 Annahme oder Ablehnung von Zertifikatsanfragen

Der vom Antragsteller 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 für Server beantragen kann, die zuvor bei der Registrierungsstelle für ihn registriert wurden. Dies geschieht im Regelfall innerhalb der Web-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)

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

Die Endstellen-Zertifizierungsstellen der SSL-PKI unterliegen Technischen Einschränkungen, weshalb keine Verpflichtung besteht, CAA zu nutzen.

4.3 Zertifikatserstellung

4.3.1 Aufgaben der Zertifizierungsstellen

Von der Zertifizierungsstelle sollen Zertifikatsanträge bearbeitet werden.

Die ordnungsgemäße Erstellung der beantragten Zertifikate soll regelmäßig von der Wurzel-Zertifizierungsstelle 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 Bayerischen SSL-PKI.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme des Zertifikates durch den Zertifikatsnehmer

Nach Erhalt der Zertifikate muss der Zertifikatsnehmer dieses Mate-rial 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. Eine Veröffentlichung des Zertifikates erfolgt unabhängig von der Akzeptanz durch seinen Besitzer (bzw. den Zertifikatsverantwortlichen).

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. Der Zertifikatsverantwortliche kann 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 durch den Zugriffsschutz des Betriebssystems oder durch organisatorische Maßnahmen gesichert erfolgen.

Der Zertifikatsverantwortliche darf den 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 Zertifikatserneuerung sollen vom Zertifikatsverantwortlichen gestellt werden.

4.7.3 Ablauf der Schlüsselerneuerung

Der Zertifikatsverantwortliche soll sechs Wochen vor Ende der Laufzeit über das anstehende Laufzeitende informiert werden. Der Zertifikatsverantwortliche muss sich selbständig um die rechtzeitige Erstellung und Zertifizierung der Schlüssel kümmern.

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 Zertifikatsmodifizierung 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 Zertifikatsnehmer benötigt das Zertifikat nicht mehr, weil
    - er nicht mehr für den Server 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
    - der im Zertifikat verwendete DNS-Name an eine andere Person vergeben wurde oder
    - das Zertifikat nicht bestimmungsgemäß verwendet wurde.
- Die Angaben im Zertifikat sind nicht mehr gültig. (z.B. Änderung des DNS-Namens)
- Der private Schlüssel wurde verloren oder kompromittiert.
- Die Zertifizierungsstelle hat festgestellt, dass 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 die Zertifizierungsstelle fallen 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. kann das CA/Browser Forum feststellen, dass ein nicht mehr empfohlener kryptographischer/ Signaturalgorithmus oder Schlüsselgröße ein nicht akzeptierbares Risiko sind, und dass solche Zertifikate dementsprechend innerhalb einer gegebenen Zeitdauer von der Registrierungsstelle oder der Zertifizierungsstelle widerrufen und ersetzt werden sollten.)

4.9.2 Wer kann einen Widerrufsantrag stellen

Einen Widerrufsantrag darf stellen:

- der Zertifikatsnehmer bzw. ein Zertifikatsverantwortlicher bei Gruppen- und Serverzertifikaten,
- der rechtliche Vertreter des Zertifikatsnehmers,
- die Registrierungsstelle,
- die Wurzelregistrierungsstelle,
- die Zertifizierungsstelle,

- die Wurzelzertifizierungsstelle.

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 Web-Schnittstelle (Web-Frontend, i.d.R. durchgehend (24x7) erreichbar, Ausnahmen entsprechend SLA),
- telefonisch beim ServiceDesk des ITDLZ im LDBV (Telefon: 089/2119-4924, entsprechend dem Servicekatalog Montag bis Freitag von 7:00 Uhr bis 18:00 Uhr erreichbar),
- persönlich bei der Registrierungsstelle.

Um einen Widerrufsantrag über die Web-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 alle 12 Stunden neu erstellt und veröffentlicht werden.

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 SSL-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 Teilnehmers 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 nicht erlaubt.

4.9.14 Wer kann einen Antrag auf temporäre Sperrung stellen

Eine temporäre Sperrung bzw. eine Suspendierung von Zertifikaten ist nicht erlaubt.

4.9.15 Verfahren zur temporären Sperrung

Eine temporäre Sperrung bzw. eine Suspendierung von Zertifikaten ist nicht erlaubt.

4.9.16 Maximale Sperrdauer bei temporärer Sperrung

Eine temporäre Sperrung bzw. eine Suspendierung von Zertifikaten ist nicht erlaubt.

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 Bayerischen SSL-PKI nicht mehr nutzen möchte oder wenn die Bayerische SSL-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 erfolgt keine Schlüsselhinterlegung (Key Backup).

4.12.2 Richtlinien und Praktiken zum Schutz und Wiederherstellung von Sitzungsschlüsseln

Sitzungsschlüssel werden nicht hinterlegt.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Physikalische Sicherheitsmaßnahmen

Die für den Betrieb der Bayerischen SSL-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.

Die Maßnahmen für den Betrieb der IT-Infrastruktur des LDBV durch das IT-DLZ entsprechen gemäß den Sicherheitsrichtlinien dem BSI IT-Grundschutz [2].

5.1.1 Standort

Das LDBV betreibt ein großes Rechenzentrum im IT-Dienstleistungszentrum mit Servern für unterschiedlichste Anwendungszwecke. Die Server können in Abhängigkeit ihres Schutzbedarfes in unterschiedlichen Schutzzonen untergebracht werden.

Das Rechenzentrum wird im 7x24h-Betrieb durch Personal überwacht. Dazu gehören u.a.

- Videoüberwachung des Geländes und Gebäudes,
- Überwachung von Sensoren bezüglich Klima, Lüftung, Temperatur, Sanitär und Elektrotechnik,
- Überwachung der Brandmeldeanlage,
- Überwachung der Wassermeldeanlage.

Das Personal kann ggf. weitere Notrufe absetzen, sofern diese nicht automatisch erfolgen, und Einsatzkräften Zugang verschaffen.

5.1.2 Physikalischer Zugang

Die Server der ausstellenden Zertifizierungsstellen befinden sich in zutrittskontrollierten Räumen des LDBV.
Der Physikalische Zugang zu Servern im Rechenzentrum ist auf Administratoren beschränkt. Diese Administratoren betreuen die eingesetzte Hardware.

5.1.3 Strom und Klima

Es gilt die allgemeine Richtlinie für das Rechenzentrum. Darin ist geregelt, dass die Stromzufuhr zu allen Servern redundant ausgelegt ist. Für Stromausfälle stehen USV’s und eine Netzersatzanlage (kraftstoffbetrieben) zur Verfügung.

Die Räume im Rechenzentrum sind automatisiert klimatisiert.

5.1.4 Wasser

Es gilt die allgemeine Richtlinie für das Rechenzentrum. Darin ist geregelt, dass eine Wasserwarnanlage installiert ist.

5.1.5 Brandschutz und -bekämpfung

Es gilt die allgemeine Richtlinie für das Rechenzentrum. Darin ist geregelt, dass eine Brandmeldeanlage installiert ist.

5.1.6 Verwaltung von mobilen Datenträgern

Mobile Datenträger müssen verschlossen oder vor unbefugtem Zugriff geschützt, aufbewahrt werden. Details sind im Betriebshandbuch [1] geregelt.

5.1.7 Entsorgung

Es gilt die allgemeine Sicherheitsrichtlinie für das Rechenzentrum.

Die Administratoren sind darauf hingewiesen worden, dass Server aus dem Bereich PKI besonders schutzwürdig sind. Bei Entsorgung muss sichergestellt werden, dass Daten, insbesondere Personendaten, sicher gelöscht wurden.

5.1.8 Backup an einem andere Standort

Ein Backup an einem anderen Standort ist nicht vorhanden.

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.

5.2.1 Vertrauenswürdige Rollen

Folgende sicherheitsrelevante Rollen sind festzulegen:

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

Das LDBV als Betreiber der Bayerischen Verwaltungs-PKI richtet den PKI-Betrieb und die Wurzelregistrierungsstelle ein. Die Wurzelregistrierungsstelle richtet die Zertifizierungs- und Registrierungsstellen ein. Die Wurzelregistrierungsstelle identifiziert und autorisiert die PKI-Administratoren bzw. Mitarbeiter der nachgeordneten Registrierungsstellen. Die Auditoren werden von der Wurzel-Zertifizierungsstelle benannt.

5.2.2 Anzahl an Personen, die für bestimmte Aufgeben benötigt werden

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.

5.2.3 Identifizierung und Authentifizierung für jede Rolle

Die Identifizierung an Servern erfolgt i.d.R. durch Nutzername und Passwort. Es gilt die allgemeine Richtlinie für das Rechenzentrum, in der u.a. die Passwort-Policy geregelt ist.

Die Identifizierung am HSM erfolgt durch personengebundene Admin-USB-Token.

Die Identifizierung für Konfigurationsänderungen in der CA erfolgt durch Smartcards. Alle Änderungen (z.B. an Zertifizierungsstellen und Zertifikatsvorlagen) sind nur im 4-Augen-Prinzip möglich.

Die Identifizierung der PKI-Rollen (Wurzel-RA, RA, Administrator, Antragsteller) am Web Frontend der Zertifizierungsstelle erfolgt durch Nutzername und Passwort.

5.3 Personelle Sicherheitsmaßnahmen

Die Administratoren und die Mitarbeiter der Wurzelregistrierungsstelle und der nachgeordneten Registrierungsstellen werden vom LDBV geschult, bevor sie ihre Arbeit aufnehmen. Neue Mitarbeiter einer bestehenden Registrierungsstelle sind vom LDBV zeitnah zu schu-

len. Auffrischungskurse und Schulungen aufgrund größerer Änderungen müssen nach Bedarf angeboten werden.

5.3.1 Anforderungen an Qualifikationen, Erfahrung und Berechtigungen

Neue PKI-Administratoren werden durch geeignete Schulungen und Einweisungen durch Kollegen eingearbeitet.

Trustcenter-Mitarbeiter (Wurzel-RA) werden durch Schulungen und Einweisungen durch PKI-Administratoren eingearbeitet.

Verantwortliche und Mitarbeiter von Registrierungsstellen sind verpflichtet, die vom LDBV angebotene Schulung zu besuchen.

Mitarbeiter des ServiceDesks werden durch das Trustcenter (Wurzel-RA) in ihre Aufgaben eingewiesen.

5.3.2 Prüf-Prozeduren im Hintergrund

Für alle Mitarbeiter des LDBV werden bei Einstellungen

- die Qualifikationen überprüft (Schulische Bildung, Ausbildung, ggf. Fortbildungen, ggf. Arbeitszeugnisse) und
- eine Sicherheitsüberprüfung (inkl. Abfrage polizeiliches Führungszeugnis) durchgeführt.

5.3.3 Anforderungen an Ausbildung

Personen, die im Bereich PKI arbeiten, müssen fachliche Mindestanforderungen erfüllen. Je nach Einsatzgebiet können das technisches Wissen und Erfahrung sein, oder auch Erfahrung mit Datenschutz und Datensicherheit z.B. aus dem Bereich der Personalsachbearbeitung.

Neue Mitarbeiter im Bereich PKI-Technik und Trustcenter erhalten eine ausführliche Einarbeitung mit sukzessiven Aufgaben- und Rechte-Erweiterungen.

Mitarbeiter von Registrierungsstellen erhalten eine Schulung durch Mitarbeiter des LDBV.

5.3.4 Häufigkeit und Anforderungen für Fortbildungen

Alle Beteiligten an der PKI sollten regelmäßig an Fort- und Weiterbildungen teilnehmen.

5.3.5 Häufigkeit und Anforderungen für Job Rotation

Keine Festlegung.

5.3.6 Sanktionen für unautorisierte Aktionen/Aktivitäten

Angemessene Sanktionen gemäß Betriebshandbuch [1] werden für unautorisierte Aktionen/ Aktivitäten verhängt.

5.3.7 Anforderungen an unabhängige Dienstleister

Zu externen Dienstleistern dieser PKI zählen ausschließlich Registrierungsstellen und deren Mitarbeiter. Diese Mitarbeiter werden durch das LDBV geschult. Die im LDBV angesiedelte Wurzel-Registrierungsstelle überwacht die Tätigkeiten der Registrierungsstellen.

5.3.8 Dem Personal zur Verfügung stehende Dokumentationen

Dokumentationen für PKI-Administratoren sind hauptsächlich technische Handbücher für Hard- oder Software, außerdem Betriebshandbuch [1], Architekturkonzept [1a], Sicherheitskonzept [1b], Backup-Recovery-Konzept [1c].

Dokumentationen für Registrierungsstellen und Anwender werden durch PKI-Administratoren und/oder Trustcenter-Mitarbeiter erstellt, weiterentwickelt und im Internet veröffentlicht.

5.4 Sicherheitsüberwachung

Im Sicherheitskonzept [1b] sind zu überwachende Ereignisse so zu definieren, dass Verstöße gegen die vorliegende Zertifizierungsrichtlinie 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 sollten mindestens arbeitstäglich überprüft und ausgewertet werden.

Alle Komponenten der Bayerischen SSL-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 Regelungen 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 Regelungen für den Zertifizierungsbetrieb. Die Überprüfung erfolgt durch die Auditoren.

5.5 Archivierung

Folgende Daten müssen von der Wurzelregistrierungsstelle archiviert werden:

- Alle Anträge, die eine Registrierungs- oder Zertifizierungsstelle betreffen.

Alle Anträge zu Registrierungs- und Zertifizierungsstellen sind so lange zu archivieren, wie die Registrierungs- bzw. Zertifizierungsstelle besteht und danach für weitere sieben 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 Bayerischen Verwaltungs-PKI teilnimmt und danach für weitere sieben Jahre.

Folgende Daten müssen von der Zertifizierungsstelle der Bayerischen SSL-PKI archiviert werden:

- Zertifikate der Zertifizierungsstellen,
- Zertifikate der Zertifikatsnehmer,
- Logfiles (Audit Log).

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 sieben Jahre archiviert werden.

Private Schlüssel von Zertifikatsnehmern dürfen archiviert werden.

5.6 Schlüsselwechsel der Zertifizierungsstelle

Ein Schlüsselwechsel soll bei einer Zertifizierungsstelle immer dann erfolgen, wenn mit dem aktuellen Schlüssel keine Zertifikate mehr ausgestellt werden können, deren Gültigkeit die Gültigkeitsdauer der CA selber übersteigt (Schalenmodell).

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

5.7 Kompromittierung einer Zertifizierungsstelle und Wiederherstellung

5.7.1 Kompromittierung

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 sind ebenfalls zu widerrufen. Die betroffenen Benutzer sind geeignet zu informieren.

Im Zertifizierungsprozess für eine Zertifizierungsstelle erhält die Wurzelzertifizierungsstelle:

- ein Sperrpasswort und
- die Namen, Telefonnummern und E-Mail Adressen der Sperrberechtigten für diese Zertifizierungsstelle.

Einer der Sperrberechtigten muss die Sperrung unverzüglich bei der Wurzelzertifizierungsstelle einreichen. Dafür hat er/ sie folgende Möglichkeiten:

- Telefon,
- Telefax oder
- E-Mail.

Die Wurzel-Zertifizierungsstelle wird danach den Betreiber der Zertifizierungsstelle (LDBV) telefonisch kontaktieren (Hauptnummer aus dem Telefonbuch) und sich mit mind. einem Sperrberechtigten in Verbindung setzten. Der/ die Sperrberechtigte muss das Sperrpasswort sagen.

Entsprechend [4] unternimmt die Wurzelzertifizierungsstelle im kommerziellen Rahmen akzeptable Maßnahmen, um das Zertifikat zügig nach Eingang und erfolgreicher Validierung eines Widerrufsantrags zu sperren. Eine neue Sperrliste wird sofort ausgestellt und veröffentlicht.

5.7.2 Wiederherstellung

Nach einer Kompromittierung kann die PK-Infrastruktur unter bestimmten Rahmenbedingungen wieder neu eingerichtet werden.

Zunächst müssen die Ursachen für eine Kompromittierung gefunden werden.

Technische Fehler müssen überarbeitet und beseitigt werden.
Menschliche Fehler müssen durch Maßnahmen, Regelungen u.ä. auf ein minimales Risiko reduziert werden.
Die genauen Maßnahmen sind im Sicherheitskonzept [1b] definiert. Externen Betriebsprüfern kann zu diesem Dokument Einsicht gewährt werden.

Vor einer Wiederaufnahme des PKI-Betriebes:

- sollte die Technische Umgebung erneut auf maximal mögliche Sicherheit überprüft werden und
- muss die Zertifizierungsstelle mit neuem Schlüsselmaterial ausgestattet werden.

5.8 Auflösen einer Zertifizierungsstelle

Wird eine Zertifizierungsstelle aufgelöst, so müssen das Zertifikat dieser Zertifizierungsstelle und alle von ihr ausgestellten Zertifikate 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 regelt das Betriebshandbuch [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 für Zertifikatsnehmer 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

Es werden keine privaten Schlüssel übertragen.

6.1.3 Übermittlung des öffentlichen Schlüssels an Zertifikatsaussteller

Der Antragsteller schickt 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 Bayerischen Infrastruktur-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 für den Gültigkeitszeitraum vom BSI [5] als sicher eingestuft sind und dem FIPS-Standard [6] genügen. 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.

6.1.6 Parameter der öffentlichen Schlüssel und Qualitätssicherung

Die Qualität der erzeugten Public Key Parameter der Zertifizierungsstelle der Bayerischen SSL-PKI sollten den vom BSI als geeignet eingestufte Kryptoalgorithmen [5] entsprechen. In besonderen Fällen, können die Empfehlungen des BSI als nicht bindend für die Bayerische Infrastruktur-PKI betrachtet werden. Dazu gehören beispielsweise Kompatibilitätsprobleme bei Clients, die dem Standard nach BayITS-11 [7] entsprechen und daher weit verbreitet sind.

6.1.7 Schlüsselverwendungszwecke und Beschränkungen

Zertifizierungsstelle:

Die Zertifizierungsstelle der SSL-PKI gilt als Technisch Beschränkt im Sinne der Baseline Requirements des CAB Forums [3]. Daraus folgen Anforderungen an verschiedene Zertifikatserweiterungen.

Das Zertifikat der Zertifizierungsstelle der Bayerischen SSL-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 Erweiterte Schlüsselverwendung (X.509v3 ExtendedKeyUsage extension) wird als nicht-kritisch markiert. In dieser Erweiterung müssen alle Schlüsselverwendungszwecke eingetragen werden, für die die CA Endstellenzertifikate ausstellt.

Die ebenfalls als kritisch markierten Basiseinschränkungen (X.509v3 BasicConstraints extension) machen deutlich, dass es sich um ein Zertifikat einer Zertifizierungsstelle handelt.

Des Weiteren enthält das Zertifikat der Zertifizierungsstelle eine als nicht-kritisch markierte Erweiterung zu Namenseinschränkungen (X.509v3 NameConstraints extension). Hier werden URI's erlaubt oder verboten.

Endstellen:

Die 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.

Jedes eingesetzte CA-Produkt bietet verschiedene Zertifikatstemplates an, die sich u.a. im Verwendungszweck unterscheiden können. Diese Policy erlaubt Templates für:

- Web-Server (Mix mit SSL-Server).

6.2 Schutz des Privaten Schlüssels und Einsatz von Kryptographischen Modulen

Die Schlüssel der Zertifizierungsstelle der Bayerischen SSL-PKI müssen 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).

Jeder Zertifikatsverantwortliche muss seine(n) privaten Schlüssel vor Verlust, Veränderung und fremdem Zugriff schützen.

6.2.1 Standards des kryptographischen Moduls

Das bei der Zertifizierungsstelle eingesetzte kryptographische Modul besitzt eine Sicherheitszertifizierung nach FIPS 140-2 Level 3.

6.2.2 Teilung des privaten Schlüssels

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

6.2.3 Hinterlegung des privaten Schlüssels

Die privaten Schlüssel der Zertifizierungsstellen der Bayerischen SSL-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 Bayerischen SSL-PKI befinden sich im HSM und müssen mit Sicherungsmethoden des HSM-Herstellers gesichert werden.

Ein zentrales Backup privater Endanwenderschlüssel erfolgt nicht. Zertifikatsnehmer dürfen ihre Schlüssel selbst sichern, sofern der Schutz des privaten Schlüssels nicht gelockert oder gelöst wird.

6.2.5 Archivierung des privaten Schlüssels

Keine Festlegung.

6.2.6 Transfer des privaten Schlüssels in oder aus einem kryptographischen Modul

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

6.2.7 Speicherung des privaten Schlüssels in einem kryptographischen Modul

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

6.2.8 Aktivierung des privaten Schlüssels

Zum Aktivieren des privaten Schlüssels der Zertifizierungsstelle für die Zertifizierung von Schlüsseln für nachgeordnete Zertifizierungsstellen genügt die Eingabe eines Passwortes beim Start des Zertifizierungsdienstes auf dem CA-Server. Das benötigte Passwort ist nur autorisierten PKI-Administratoren bekannt. Es wird verschlüsselt in einer Konfigurationsdatei abgelegt. Alle Konfigurationsdateien sind mit System-Zugriffsrechten geschützt.

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 Zertifizierungsstellen der Bayerischen SSL-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 bleibt immer nur für eine Aktion gültig und danach wird der Schlüssel automatisch wieder deaktiviert.

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.

Das Schlüsselmaterial auf dem Hardwaretoken muss sicher gelöscht werden. Das genaue Verfahren hängt vom eingesetzten Token ab und wird im Betriebshandbuch [1] festgelegt.

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 Bayerischen SSL-PKI zertifiziert wurden, werden in der Datenbank der Zertifizierungsstelle archiviert.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

In der SSL-PKI gelten folgende maximalen Zertifikatsgültigkeiten:

- Zertifikat der Wurzel-CA von QuoVadis: 20 Jahre
- Zertifikat der ausstellenden CA von LDBV: 10 Jahre
- Serverzertifikate: 3 Jahre (ab 1.3.2018 2 Jahre)

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

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

Der Antragsteller muss bei der Produktion des privaten Schlüssels Aktivierungsdaten (PIN, Passwort) erstellen, die den privaten Schlüssel schützen.

Für die 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

Alle PC- und Serversysteme, die im Rahmen dieser Zertifizierungsrichtlinie an der PKI teilnehmen, müssen bestimmte Sicherheitsstandards erfüllen. Dazu gehören:

- aktueller Stand des Betriebssystems (aktuelle Sicherheitspatches usw.),
- Virenscanner (PC: Schutz vor Keyloggern),
- Benutzerauthentifizierung beim Anmelden am Betriebssystem.

Bei Servern zusätzlich:

- 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.

Diese Vorgaben entsprechen den allgemeinen Richtlinien für Server des LDBV/ IT-DLZ.

6.5.2 Güte der Sicherheitsmaßnahmen

Es 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.

Betriebssystemaktualisierungen und neue Programmversionen müssen vor dem Einspielen in die Betriebsumgebung funktionalen und qualitätssichernden Tests unterzogen werden.

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

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 sind im Betriebshandbuch [1] bzw. im Sicherheitskonzept [1b] beschrieben. Dazu gehört u.a. dass

- PKI-Server in einem eigenen Netzwerkbereich untergebracht und durch Firewalls von anderen Systemen abgeschottet sind,
- dass nicht benötigte Netzwerkports deaktiviert sind,
- dass Kommunikationsverbindungen zu anderen Servern entweder durch PKI-Software oder durch Software, die zum Betrieb eines Servers notwendig ist (z.B. Betriebssystemupdates, Sicherungssoftware usw.), benötigt werden.

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 und dienen den in 6.1.7 genannten Verwendungszwecken.

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.

7.4 LDAP Profile

Die eingesetzten LDAP Verzeichnisdienste sind nach den Standards LDAP v3 und RFC 4510 konfiguriert.

8 Konformitätsprüfung

Die Arbeitsprozesse der Zertifizierungsstellen sollen 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 die Wurzel-Zertifizierungsstelle oder durch eine von der Wurzel-Zertifizierungsstelle beauftragte Stelle erfolgen.

8.3 Verhältnis von Prüfer zu Überprüftem

Selbstüberprüfungen sind zulässig.

Erfolgt eine Prüfung durch einen unabhängigen Prüfer, darf dieser nicht gleichzeitig ein Mitglied der zu überprüfenden Stelle sein. Unter einer Stelle wird in diesem Zusammenhang eine Behörde, eine Abteilung, ein Referat 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 Zertifizierungsstelle veranlassen.

8.6 Veröffentlichung der Ergebnisse

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

9 Rechtliche Vorschriften

9.1 Gebühren

Es werden keine Gebühren erhoben.

9.2 Finanzielle Verantwortung

Die finanzielle Verantwortung für das LDBV trägt der Freistaat Bayern. Er haftet für sämtliche Verbindlichkeiten.

Darüber hinaus ist der Freistaat Bayern insolvenzunfähig. Gem. § 12 Abs. 1 Nr. 1 InsO ist die Eröffnung des Insolvenzverfahrens über das Vermögen eines Landes unzulässig.

9.3 Vertraulichkeit von Informationen

Alle Informationen, die nicht vom LDBV oder einer anderen Behörde veröffentlicht werden, werden vertraulich behandelt.

Beamtinnen und Beamte haben gem. § 37 Abs. 1 BeamtStG über die ihnen bei oder bei Gelegenheit ihrer amtlichen Tätigkeit bekannt gewordenen dienstlichen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt auch über den Bereich eines Dienstherrn hinaus sowie nach Beendigung des Beamtenverhältnisses. Angestellte des öffentlichen Diensts sind gem. § 3 Abs. 2 TV-L zur Verschwiegenheit verpflichtet.

9.4 Datenschutz

Das LDBV und die anderen beteiligten Behörden beachten alle gesetzlichen Bestimmungen über den Datenschutz.

Personenbezogene Daten werden an Dritte nur im Rahmen vertraglicher Regelungen oder aufgrund einer gesetzlichen Verpflichtung weitergegeben.

9.5 Urheberrechte

Es gelten die gesetzlichen Bestimmungen zum Urheberrecht. In dieser Zertifizierungsrichtlinie werden keine vom Gesetz abweichenden, besonderen Regelungen getroffen.

9.6 Gewährleistung

Es gelten die gesetzlichen Gewährleistungsvorschriften.

9.7 Gewährleistungsausschluss

Ein Gewährleistungsausschluss ist nicht vereinbart.

9.8 Haftungsbeschränkung

Die Haftung wird ausgeschlossen. Dies gilt nicht für

1. Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit oder für vorsätzlich, die auf einer fahrlässigen Pflichtverletzung beruhen und

2. sonstige Schäden, die auf einer grob fahrlässigen oder vorsätzlichen Pflichtverletzung beruhen.

9.9 Haftungsfreistellung

Eine Haftungsfreistellung erfolgt nicht.

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.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

In dieser Zertifizierungsrichtlinie werden keine entsprechenden Regelungen getroffen.

9.12 Änderungen/Ergänzungen der Richtlinien

Änderungen und Ergänzungen der Zertifizierungsrichtlinie werden vom LDBV vorgeschlagen und mit dem StMFLH als Auftraggeber abgestimmt. Die Wurzel-Zertifizierungsstelle wird nur bei gravierenden Änderungen einbezogen und ansonsten informiert.

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

Ein Schiedsverfahren im Sinne von §§ 1025 ff. ZPO ist nicht vorgesehen.

9.14 Gerichtsstand

Es gilt der gesetzliche Gerichtstand.

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
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYBN	Bayerisches Behördennetz
CA	*Certification Authority*, Zertifizierungsinstanz
CAB	*CA/Browser-Forum*, Konsortium aus CA-Betreibern und Entwicklern von Betriebssystemen, Webbrowsern und anderer Applikationen, die Zertifikate nutzen https://cabforum.org/
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 oder Server)
FQDN	*Fully Qualified Domain Name*, Voller Servernamen inkl. Domänenname
Hardwaretoken	Ein Hardwaretoken ist eine Hardware zur Speicherung von privaten Schlüsseln, die u. a. eine unberechtigte Nutzung des privaten Schlüssels verhindert.
Interner Servername	*Internal Server Name*, Servername (mit oder ohne nicht-registrierten Domain Name) der nicht im öffentliche DNS auflösbar ist.
IT-DLZ	*IT-Dienstleistungszentrum*, ein Betriebsteil des LDBV und Betreiber der bayerischen SSL-PKI
HSM	Hardware Security Module, an den CA-Server angeschlossenes Modul zur sicheren Aufbewahrung von Verschlüsselungs- und Signaturschlüsseln der CA
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*

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
PIN	*Personal Identification Number*, geheime Zahl- oder Zeichenfolge (z.B. um den privaten Schlüssel zu schützen)
PSE	*Personal Security Environment* (z.B. passwortgeschützte P12 Datei)
RA	*Registration Authority*, Registrierungsstelle
Registrierungsstelle	Stelle, die eine Person als Teilnehmer registriert und identifiziert
Reservierte IP-Adresse	*Reserved IP Address*, eine IPv4 oder IPv6-Adresse, die die IANA als reserviert markiert hat: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
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.
RFC-822 Name	E-Mail Adresse
Root-CA	vgl. Wurzel-CA
SAN	Subject Alternative Name
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.
SLA	*Service Level Agreement* (Vereinbarung über den Betrieb & Verfügbarkeit von Servern zwischen Server- und PKI-Administratoren)
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, für Landesentwicklung und Heimat*, dem LDBV übergeordnete Dienststelle und Auftraggeber der Bayerischen Infrastruktur-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)
USV	Unterbrechungsfreie Stromversorgung, Batteriesystem, welches die Stromzufuhr für Server während eines Stromausfalls o.ä. für einen kurzen Zeitraum sichert
Widerrufsliste	(siehe Sperrliste)
Wildcard-Zertifikat	Zertifikat das in einem Teil eines FQDN einen Stern (*) trägt und somit für mehrere Instanzen genutzt werden kann
Wurzel-CA	(auch Wurzelzertifizierungsstelle) 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] Betriebskonzept für die Bayerische Verwaltungs-PKI
damit zusammenhängende Dokumente:

- [1a] Architekturkonzept
- [1b] Sicherheitskonzept
- [1c] Backup-Recovery-Konzept

[2] BSI, IT Grundschutzhandbuch
http://www.bsi.de/gshb/

[3] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“ oder “Baseline Requirements”
http://www.cabforum.org

[4] CP/CPS der QuoVadis Wurzel-CA
https://www.quovadisglobal.bm/~/media/Files/Repository/QV_RCA1_RCA3_CPCPS_V4_10.ashx

[5] BSI, Technische Richtlinie (BSI TR-02102-1), Kryptographische Verfahren: Empfehlungen und Schlüssellängen
http://www.bsi.de/

[6] FIPS (Federal Information Processing Standard), US-Gremium, welches Standards entwickelt; im Dokument wird FIPS 140-2 (Sicherheitsanforderungen für Kryptographische Module) verwendet
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[7] BayITS-11, IT-Standards für die Bayerische Verwaltung