Bayerisches Landesamt für
Statistik und Datenverarbeitung

Mit Bayern rechnen.

Zertifizierungsrichtlinie der Public Key Infrastructure der Bayerischen Verwaltung

für die

X.509-Zertifizierungshierarchie der Bayerischen Infrastruktur-PKI

Version 2.2
(K. Ehrhardt)
München | 25.03.2010

Änderungshistorie:

Version	Datum	Bearbeiter	Bemerkung
1.0	24.03.09	Fr. Ehrhardt	Freigabe der Version 1.0 und Veröffentlichung
2.0	21.01.10	Fr. Ehrhardt	Änderung der Infrastruktur (Einführung einer übergeordneten Wurzel-CA)
2.1	04.03.10	Fr. Ehrhardt	Kleinere Änderungen (u.a. 6.1.6)
2.2	25.03.10	Fr. Ehrhardt	Kapitel 4.6 überarbeitet

Inhaltsverzeichnis:

1 Einführung

Das Bayerische Landesamt für Statistik und Datenverarbeitung (LfStaD) betreibt im Auftrag des Bayerischen Staatsministeriums des Innern 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 LfStaD 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 LfStaD betriebene PKI besteht aus mehreren eigenständigen Zertifizierungshierarchien.

Gegenstand dieser Zertifizierungsrichtlinie ist die Zertifizierungshierarchie, deren Wurzel (Root) vom LfStaD betrieben wird und die ausschließlich Zertifikate für technische Infrastrukturen erstellen (im Folgenden Infrastruktur-Zertifikate genannt).

- Das LfStaD betreibt die Wurzel-CA. Diese CA zertifiziert nachgeordnete Sub-CA's der Bayerischen Verwaltung.
- Das LfStaD betreibt zwei Sub-CA's im Active Directory des Bündnisforests.
- Weitere Sub-CA's können von anderen Behörden in der staatlichen und kommunalen Verwaltung Bayerns betrieben werden.

Die vorliegende Zertifizierungsrichtlinie ist verpflichtend für alle Betreiber einer Zertifizierungsstelle innerhalb der Bayerischen Infrastruktur-PKI in der staatlichen und kommunalen Verwaltung Bayerns.

Die nach der vorliegenden Zertifizierungsrichtlinie betriebenen Public Key Infrastrukturen werden im Folgenden als Bayerische Infrastruktur-PKI bezeichnet.

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 Bayerischen Infrastruktur-PKI und soll dem Leser ein allgemeines Verständnis der Bayerischen Infrastruktur-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.

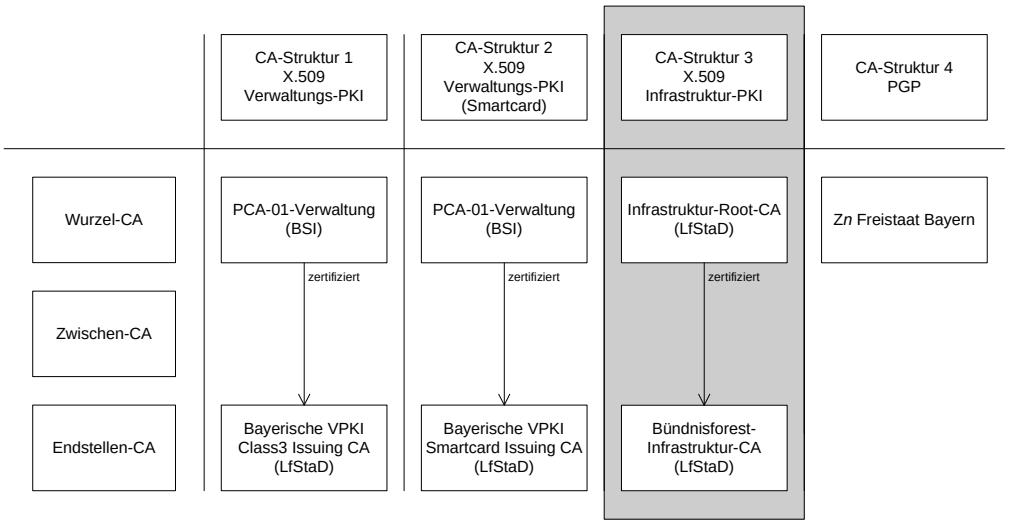
1.1.2 Aufbau der Bayerischen Infrastruktur-PKI

Die Bayerische Verwaltungs-PKI besteht aus mehreren, voneinander unabhängigen Zertifizierungshierarchien nach X.509 und einer Zertifizierungshierarchie für PGP-Schlüssel nach OpenPGP. 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 Infrastrukturzertifikate in der staatlichen und kommunalen Verwaltung Bayerns zur Verfügung stellt. Sie ist nicht Teil der Deutschen Verwaltungs-PKI, die vom BSI betrieben wird.

Die Bayerische Verwaltungs-PKI besteht aus mehreren, voneinander unabhängigen Zertifizierungshierarchien nach X.509 und einer Zertifizierungshierarchie für PGP-Schlüssel nach OpenPGP. 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 Infrastrukturzertifikate 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 Infrastruktur-PKI

Version: 2.2

Datum: 25.03.2010

Identifier: 1.3.6.1.4.1.19266.1.2.2

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen

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

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

1.3.2 Registrierungsstellen

Registrierungsstellen sind nicht vorgesehen. Die Registrierung wird durch die Zertifizierungsstelle vorgenommen.

1.3.3 Zertifikatsnehmer

Zertifikate und Schlüssel werden für die staatliche und kommunale Verwaltung in Bayern oder Dienstleister in deren Auftrag ausgegeben.

Zertifikatsnehmer sind automatisierte IT-Prozesse (z.B. Zertifizierungsstelle, elektronische Stempel, Serverprozesse mit Signatur, SSL-Server).

1.3.4 Zertifikatsprüfer

Zertifikatsprüfer überprüfen anhand eines Zertifikates der Bayerischen Infrastruktur-PKI die Authentizität 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 Infrastruktur-PKI

Die Schlüssel und Zertifikate dürfen als Infrastrukturzertifikate für automatisierte IT-Prozesse (z.B. elektronische Stempel, Serverprozesse mit Signatur, SSL-Server) eingesetzt werden.

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

1.4.2 Verbotene Verwendungszwecke innerhalb der Infrastruktur-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 [1] werden durch das LfStaD verwaltet. Änderungen an der Zertifizierungsrichtlinie werden im Abschnitt Änderungshistorie zu Beginn des Dokumentes protokolliert. Änderungen an der Zertifizierungsrichtlinie müssen vom StMI genehmigt werden.

1.5.2 Ansprechstelle

Bayerisches Landesamt für Statistik und Datenverarbeitung
- Trustcenter -
Neuhauser Straße 8
80331 München

Telefon: 089/2119-924
Fax: 089/2119-1873
E-Mail: trustcenter@lfstad.bayern.de

1.5.3 Eignungsprüfer für Regelungen zum Zertifizierungsbetrieb gemäß Zertifizierungsrichtlinie

StMI

1.5.4 Verfahren zur Anerkennung von Regelungen zum Zertifizierungsbetrieb

Die Regelungen zum Zertifizierungsbetrieb sind dem StMI vorzulegen. Das StMI entscheidet anschließend über den Zertifizierungsbetrieb.

1.6 Definitionen und Abkürzungen

Siehe Glossar

2 Veröffentlichungen und Verzeichnisdienst

2.1 Verzeichnisdienst

Die Wurzel-Zertifizierungsstelle stellt die von ihr 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 über OCSP ist zusätzlich zulässig.

Die Zertifikate der Wurzel-Zertifizierungsstelle sollen im Verzeichnisdienst in dem durch den Namen der Zertifizierungsstelle 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:

- Für jede Zertifizierungsstelle ihr Zertifikat und dessen Fingerabdruck,
- Zertifizierungsrichtlinie,
- Aktuelle Sperrlisten.

2.3 Aktualisierung der Informationen

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 anonym erfolgen. 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.

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. einen Benutzer (User Principal Name, UPN) oder 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 eines Zertifikats für Zertifizierungsstellen müssen im DName die Bestandteile „countryName“ und „organizationName“ enthalten sein.
- Im Attribut subject eines Zertifikats für Endstellen müssen im DName die Bestandteile „commonName“ (cn), „organizationalUnitName“ (ou), „organizationName“ (o) und „CountryName“ (c) enthalten sein.

3.1.2 Aussagekraft von Namen

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

- Zertifikate für automatisierte IT-Prozesse dürfen nicht auf die Namen von natürlichen oder juristischen Personen ausgestellt werden.
- Der Name der Serverinstanz muss eindeutig hervorgehen.

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

3.1.3 Anonyme und Pseudonyme

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

3.1.4 Namensinterpretation

Keine Festlegung.

3.1.5 Eindeutigkeit von Namen

Die Eindeutigkeit von Namen muss von der Zertifizierungsstelle gewährleistet 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 Infrastruktur-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 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 (automatisierten IT-Prozessen)

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

Ist eine Zertifizierungsstelle in ein Active Directory integriert, ist es ausreichend, wenn der IT-Prozess ebenfalls Mitglied des gleichen Domänenverbundes ist. Er gilt damit als authentifiziert und „darf“ Zertifikate beantragen.

3.2.3 Authentifikation von natürlichen Personen

Keine Festlegung.

3.2.4 Nicht überprüfte Teilnehmerangaben

Keine Festlegung.

3.2.5 Überprüfung der Berechtigung

Keine Festlegung.

3.2.6 Interoperabilitätskriterien

Keine Festlegung.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Bei einer Zertifikatserneuerung muss die Zertifizierungsstelle die Authentifizierung des IT-Prozesses erneut prüfen.

3.3.2 Zertifikatserneuerung nach einem Zertifikatswiderruf

Nach einem Zertifikatswiderruf muss ein Neuantrag gestellt werden.

3.4 Identifizierung und Authentifizierung bei einem Widerruf

Ein Antrag auf Zertifikatswiderruf soll durch einen Administrator des betroffenen IT-Prozesses erfolgen. Die Authentifizierung erfolgt an Hand der Person des Administrators.

Ein CA-Adminstrator (Verantwortlicher) soll in begründeten Fällen (z. B. bei Verstößen gegen die Sicherheitsrichtlinie) auch ohne Antrag eines Administrators Zertifikate widerrufen können.

4 Ablauforganisation

4.1 Zertifikatsantrag

4.1.1 Wer kann einen Zertifikatsantrag stellen

Bei der Wurzel-Zertifizierungsstelle dürfen ausschließlich nachgeordnete Sub-CA's Zertifikatsanträge einreichen.

Bei einer Sub-CA dürfen ausschließlich IT-Prozesse (Server, Maschine) Zertifikate beantragen. Sub-CA's dürfen ihre Dienstleistungen weiter beschränken, z.B. auf bestimmte Netze.

4.1.2 Prozess und Verantwortung

Antragsteller beantragen ihre benötigten Zertifikate direkt bei der Zertifizierungsstelle. Das genaue Antragsverfahren ist u.a. abhängig vom eingesetzten CA-Produkt und wird von der Zertifizierungsstelle festgelegt und in den Regelungen zum Zertifizierungsbetrieb [1] festgeschrieben.

Wurde ein IT-Prozess (Server, Maschine) nach Kapitel 3.2.2 authentisiert, dürfen die benötigten Zertifikate für ihn beantragt werden.

Mit der Antragstellung akzeptiert der Antragsteller (Administrator des IT-Prozesses (Server, Maschine)) die Zertifizierungsrichtlinien.

Von der Wurzel-Zertifizierungsstelle sollen ausschließlich Zertifikatsanträge mit dezentraler Schlüsselerzeugung bearbeitet werden.

Nachgeordnete Zertifizierungsstellen dürfen Zertifikatsanträge mit zentraler oder dezentraler Schlüsselerzeugung bearbeiten. Diese Zertifizierungsstellen dürfen ihre Dienstleistung weiter beschränken.

4.2 Bearbeitung von Zertifikatsanträgen

4.2.1 Durchführung von Identifikation und Authentifizierung

Zertifikatsanträge werden bei Eingang durch die Zertifizierungsstelle geprüft. Die Überprüfung darf manuell oder automatisiert erfolgen. Es dürfen nur Zertifikatsanträge von autorisierten Antragstellern mit einem Zertifikat beantwortet werden.

Zertifikatsnehmer der Wurzel-Zertifizierungsstelle müssen bei Antragstellung ein Formular [2] ausfüllen. Darin werden Kontaktdaten eines Verantwortlichen für die nachgeordnete Zertifizierungsstelle angegeben und die Einhaltung der Zertifizierungsrichtlinien bestätigt.

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.

4.2.3 Bearbeitungsdauer

Die Zertifikatsanträge sollen von der Zertifizierungsstelle spätestens innerhalb von 5 Werktagen nach Antragseingang bearbeitet werden.

4.3 Zertifikatserstellung

4.3.1 Aufgaben der Zertifizierungsstellen

Wurzel-Zertifizierungsstelle

Von der Wurzel-Zertifizierungsstelle sollen ausschließlich Zertifikatsanträge mit dezentraler Schlüsselerzeugung bearbeitet werden.

Die Wurzel-Zertifizierungsstelle stellt nach erfolgreicher Überprüfung des Zertifikatsantrags das Zertifikat aus und sendet dieses inklusive ihrer eigenen Zertifikate an den Antragsteller (Verantwortlicher/Administrator einer nachgeordneten Zertifizierungsstelle) zurück.

Der Name des Antragstellers und seine Organisationseinheit werden dabei aus dem Antragsformular ausgelesen.

Der Operator an der Root-CA, der den Zertifikatsantrag bearbeitet (prüft), achtet darauf, dass alle von der Root-CA ausgestellten Zertifikate den gleichen Rahmenbedingungen entsprechen.

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

Nachgeordnete Zertifizierungsstellen

Die Zertifizierungsstelle stellt nach erfolgreicher Überprüfung des Zertifikatsantrags das Zertifikat aus und sendet dieses inklusive aller Zertifikate im Zertifizierungspfad an den Antragsteller (Administrator eines IT-Prozesses) zurück.

Weitere Bedingungen legt die Zertifizierungsstelle in ihren Zertifizierungsrichtlinien bzw. in ihren Regelungen zum Zertifizierungsbetrieb selbst fest.

Die ordnungsgemäße Erstellung der beantragten Zertifikate und ggf. Schlüssel soll regelmäßig (mindestens alle 2 Jahre) von der Wurzel-Zertifizierungsstelle bzw. einem von ihr beauftragten Auditor überprüft werden.

4.3.2 Benachrichtigung des Antragstellers

Wird der Zertifikatsantrag abgelehnt, erhält der Antragsteller eine entsprechende Benachrichtigung. Anderenfalls erhält der Antragsteller das Zertifikat von der Zertifizierungsstelle der Bayerischen Infrastruktur-PKI.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme des Zertifikates durch den Zertifikatsnehmer

Nach Erhalt der Zertifikate muss der Zertifikatsnehmer dieses Material prüfen. Erfolgt kein Einspruch von Seiten des Zertifikatsnehmers gilt das Zertifikat als akzeptiert.

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

4.4.2 Zertifikatsveröffentlichung

Nach Erstellung der Zertifikate soll die Zertifizierungsstelle bei Bedarf 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 Administrator des IT-Prozesses hat die Verantwortung für den sachgerechten und sicheren Gebrauch des Zertifikats und des zugehörigen privaten Schlüssel zu übernehmen.

Der Administrator des IT-Prozesses 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 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 von Schlüsseln der Zertifizierungsstellen 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. Dies kann auch automatisiert erfolgen.

4.7.3 Ablauf der Schlüsselerneuerung

Die Zertifikatserneuerung entspricht einem Zertifikatsneuantrag.

Der Zertifikatsverantwortliche soll seine neuen privaten Schlüssel am eigenen Server/System (Zertifizierungsstelle) erzeugen und dann einen digitalen Zertifikatsantrag bei der Wurzel-Zertifizierungsstelle der Bayerischen Infrastruktur-PKI einreichen.

Eine erneute Registrierung ist nicht 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:

- Die Angaben im Zertifikat sind nicht mehr gültig. (z.B. Änderung des Namens)
- Der private Schlüssel wurde verloren oder kompromittiert.
- Der Zertifikatsnehmer ist nicht mehr berechtigt, ein Zertifikat zu besitzen.
- Der Zertifikatsnehmer benötigt das Zertifikat nicht mehr.
- Der Zertifikatsnehmer hält die Zertifizierungsrichtlinie nicht ein.
- Die Zertifizierungsstelle hält die Zertifizierungsrichtlinie oder die Regelungen zum Betrieb der Zertifizierungsstelle nicht ein.
- Die Zertifizierungsstelle fällt ersatzlos weg.
- Kompromittierung des privaten CA-Schlüssels.

4.9.2 Wer kann einen Widerrufsantrag stellen

Einen Widerrufsantrag darf stellen:

- der Zertifikatsnehmer (Administrator des IT-Prozesses),
- die Zertifizierungsstelle.

4.9.3 Ablauf

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

Der Administrator des IT-Prozesses muss einen Widerrufsantrag bei der Zertifizierungsstelle stellen. Hierfür muss er telefonisch oder per E-Mail die Zertifizierungsstelle kontaktieren.

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 nach Meldungseingang durch den Zertifikatsverantwortlichen (vgl. Kapitel 4.1.1) 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 höchstens 7 Tagen besitzen und mindestens täglich (alle 24 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 Wurzel-CA sollen auch auf einem OCSP-Server veröffentlicht werden. Sperrlisten nachgeordneter CA’s dürfen per OCSP publiziert 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 nicht erlaubt.

4.9.14 Wer kann einen Antrag auf temporäre Sperrung stellen

Keine Festlegung.

4.9.15 Verfahren zur temporären Sperrung

Keine Festlegung.

4.9.16 Maximale Sperrdauer bei temporärer Sperrung

Keine Festlegung.

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

4.10.1 Betriebsbedingte Eigenschaften

Sofern OCSP-Dienste eingesetzt werden, muss der Verweis auf diesen Publikationsort in die ausgestellten Zertifikate aufgenommen werden.

4.10.2 Verfügbarkeit des Dienstes

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

Wird ein OCSP-Dienst angeboten, sollten alle Zertifikatsprüfer diesen 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

Keine Festlegung.

4.11 Beendigung des Vertragsverhältnisses durch den Zertifikatsnehmer

Das Vertragsverhältnis kann beendet werden, wenn der Zertifikatnehmer die Dienste der Bayerischen Infrastruktur-PKI nicht mehr nutzen möchte oder wenn die Bayerische Infrastruktur-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

Keine Festlegung.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Physikalische Sicherheitsmaßnahmen

Die für den Betrieb der Bayerischen Infrastruktur-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-Software vornehmen. Diese Rechte sind in einem Rollenkonzept zu verankern.

Folgende sicherheitsrelevante Rollen sind festzulegen:

- Mitarbeiter der Zertifizierungsstelle,
- Auditoren.

Die Auditoren werden vom StMI benannt.

5.3 Personelle Sicherheitsmaßnahmen

Alle Mitarbeiter der Zertifizierungsstellen müssen auf die eingesetzten Komponenten geschult werden.

5.4 Sicherheitsüberwachung

In den Richtlinien für den Zertifizierungsbetrieb [1] 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 mindestens arbeitstäglich überprüft und ausgewertet werden.

Alle Komponenten der Bayerischen Infrastruktur-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 den Zertifizierungsstellen der Bayerischen Infrastruktur-PKI archiviert werden:

- Zertifikate der Zertifizierungsstellen,
- Zertifikate der Zertifikatsnehmer.

Die Zertifikate der Zertifizierungsstellen sind bis zum Ablauf ihrer Zertifikatsgültigkeit zu archivieren. Die Zertifikate der Zertifikatnehmer müssen bis zum Ablauf der Zertifikatsgültigkeit der Zertifizierungsstelle 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

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.

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.

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

6 Technische Sicherheitsmaßnahmen

6.1 Schlüsselerzeugung und Installation

6.1.1 Schlüsselerzeugung

Das Schlüsselpaar der Wurzelzertifizierungsstelle wird in einem kryptographischen Modul erstellt.

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

Die Schlüsselpaare der Zertifikatsnehmer sollten dezentral auf dem Server/System des Zertifikatsnehmers erstellt werden. Alternativ ist eine zentrale Schlüsselerzeugung in der Zertifizierungsstelle möglich.

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

6.1.2 Übermittlung des privaten Schlüssels an den Zertifikatsnehmer

Bei privaten Schlüsseln, die dezentral von den Zertifikatsinhabern selbst erzeugt werden, ist keine Übergabe von privaten Schlüsseln erforderlich.

Bei zentral erzeugten Schlüsseln ist der Transport des privaten Schlüsselmaterials von der Zertifizierungsstelle zum Zertifikatsinhaber besonders zu schützen. Dies kann beispielsweise durch einen Hardwaretoken oder bei einem Soft-PSE mittels Transport-PIN erfolgen.

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 als sicher eingestuft sind [3]. 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 Infrastruktur-PKI sollten den vom BSI als geeignet eingestufte Kryptoalgorithmen [3] 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-04 und BayITS-11 [4] entsprechen und daher weit verbreitet sind.

6.1.7 Schlüsselverwendungszwecke und Beschränkungen

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

- RAS und IAS Server,
- Domain Controller,
- Computer (802.x, IPsec),
- Web-Server (Mix mit SSL-Server).

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 Bayerischen Infrastruktur-PKI müssen nicht in einem kryptographischen Modul erstellt und gespeichert werden. Auch Schlüssel von Zertifikatsnehmern müssen nicht in Hardware erstellt und gespeichert werden.

6.2.1 Standards des kryptographischen Moduls

Keine Festlegung.

6.2.2 Teilung des privaten Schlüssels

Keine Festlegung.

6.2.3 Hinterlegung des privaten Schlüssels

Die privaten Schlüssel der Zertifizierungsstellen der Bayerischen Infrastruktur-PKI dürfen nicht hinterlegt werden.

Die Hinterlegung privater Endanwenderschlüssel ist nicht vorgesehen.

6.2.4 Backup des privaten Schlüssels

Die privaten Schlüssel der Zertifizierungsstelle der Bayerischen Infrastruktur-PKI werden durch die Backupmechanismen der Server gesichert.

Ein Backup privater Endanwenderschlüssel ist nicht vorgesehen.

6.2.5 Archivierung des privaten Schlüssels

Keine Festlegung.

6.2.6 Transfer des privaten Schlüssels in oder aus einem kryptographischen Modul

Keine Festlegung.

6.2.7 Speicherung des privaten Schlüssels in einem kryptographischen Modul

Keine Festlegung.

6.2.8 Aktivierung des privaten Schlüssels

Zum Aktivieren des privaten Schlüssels der Zertifizierungsstelle für die Zertifizierung von Schlüsseln für nachgeordnete Zertifizierungsstellen genügt das Starten des Zertifizierungsdienstes. Ebenfalls beim Dienststart wird die Signatur der Sperrlisten aktiviert.

Beim Starten der Dienste wird die PIN für den privaten Schlüssel der Zertifizierungsstelle abgefragt. Die Kenntnis über die PIN ist auf berechtigte Personen zu beschränken.

6.2.9 Deaktivierung des privaten Schlüssels

Der private Schlüssel der Zertifizierungsstellen der Bayerischen Infrastruktur-PKI wird deaktiviert, sobald der Zertifizierungsdienst auf dem CA-Server gestoppt wird.

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

Keine Festlegung.

6.3 Andere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel, die von der Zertifizierungsstelle der Bayerischen Infrastruktur-PKI zertifiziert wurden, werden in der Datenbank der Zertifizierungsstelle bis zum Ende der Laufzeit der Zertifizierungsstelle archiviert.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Zertifikate und Schlüssel für die Wurzelzertifizierungsstelle dürfen max. 10 Jahre gültig sein.

Zertifikate und Schlüssel für Zertifizierungsstellen dürfen max. 6 Jahre gültig sein.

Zertifikate und Schlüssel für Zertifikatsnehmer, die als Soft-PSE gespeichert werden, dürfen nicht länger als 1 Jahr gültig sein. Zertifikate und Schlüssel für Zertifikatsnehmer, die in Hardware (z.B. Smartcard) gespeichert werden, dürfen 4 Jahre 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

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.

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.

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 sind Penetrationstests der Betriebsumgebung durchzuführen. 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 und dienen den in 6.1.7 genannten Verwendungszwecken.

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 Zertifizierungsstellen 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 Zertifizierungsstelle erfolgen. Weitere Überprüfungen einer Zertifizierungsstelle sollen regelmäßig vorgenommen werden.

8.2 Identität des Überprüfers

Die Überprüfung der Zertifizierungsstellen muss durch das StMI oder durch eine vom StMI 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 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

Derzeit werden keine Gebühren erhoben.

9.2 Finanzielle Verantwortung

Eine Insolvenz des LfStaD oder einer anderen Behörde kann nicht eintreten, so dass eine Abdeckung der finanziellen Verantwortungen des LfStaD durch Versicherungen nicht erforderlich ist.

9.3 Vertraulichkeit von Informationen

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

9.4 Datenschutz

Das LfStaD und die anderen beteiligten Behörden 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 LfStaD und die anderen beteiligten Behörden 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.

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 LfStaD vorgeschlagen und mit dem StMI abgestimmt.

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

Das LfStaD 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 von Streitigkeiten ist das StMI zuständig.

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
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 oder Server)
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
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)
LfStaD	Landesamt für Statistik und Datenverarbeitung
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)

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.
RFC-822 Name	E-Mail Adresse
Root-CA	vgl. Wurzel-CA
RZ-Süd	Rechenzentrum Süd; ein Betriebsteil des LfStaD und Betreiber der bayerischen Infrastruktur-PKI
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
StMI	*Staatsministerium des Innern*, dem LfStaD 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)
Widerrufsliste	(siehe Sperrliste)
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] Regelungen für den Zertifizierungsbetrieb

[2] Antragsformular für ein Zertifikat der Wurzel-Zertifizierungsstelle

[3] BSI, Technische Richtlinie (BSI TR-02109), Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 1.0, 20.06.2008, http://www.bsi.de/literat/tr/tr02102/index.htm

[4] BayITS-04, IT-Standards für die bayerische Staatsverwaltung – Betriebssystem für Client – Fat Client
BayITS-11, IT-Standards für die bayerische Staatsverwaltung - PC-Arbeitsplatz - Fat Client
http://connect.juris.bybn.de/connect?docId=VVBY-VVBY000007101&uid=bystin (ausschließlich im Behörden-Intranet)