HZD
Hessische Zentrale für Datenverarbeitung

HESSEN

HESSEN PKI

Policy - Certificate Practice Statement nach RFC 3647

24.10.2018 – 06.00

Inhaltsverzeichnis

1 Einleitung

Die Hessische Zentrale für Datenverarbeitung (HZD) betreibt für die Hessische Landesverwaltung und Institutionen des Landes Hessen verschiedene digitale, zertifikatsbasierende Schlüsselinfrastrukturen (Public Key Infrastructure, kurz PKI).

Diese Schlüsselinfrastrukturen sind über die Anwendungsszenarien gegeneinander abgegrenzt. Bisher sind dies:

- Hessen-PKI
  Diese stellt vor allem Zertifikate für die sichere E-Mail-Kommunikation aus. Die Zertifikate werden sowohl für die Absicherung der internen als auch der Kommunikation mit Personen außerhalb der hessischen Landesverwaltung genutzt.
  Zudem stellt die Hessen-PKI eine begrenzte Anzahl Zertifikate für TLS-Verschlüsselung bereit.
- System-PKI
  Diese stellt Zertifikate für die IT-Infrastruktur des Landes Hessen und die Absicherung von IT-Prozessen aus.

Die genannten Schlüsselinfrastrukturen existieren parallel und werden logisch voneinander getrennt betrieben.

Die Zertifizierungsstellen der Hessen-PKI (CA-1-Hessen) werden unterhalb der Wurzelzertifizierungsstelle des Bundesamts für Sicherheit in der Informationstechnik (BSI), betrieben und integriert die Hessen-PKI in die PKI der Verwaltung (V-PKI). Die V-PKI stellt eine bundesweite zertifikatsbasierte Schlüsselinfrastruktur der öffentlichen Verwaltung (Bund, Länder, Kommunen) dar.

Die V-PKI verfügt für ihre Wurzelzertifizierungsstelle über ein selbst signiertes CA-Zertifikat. Die Zertifizierungsstelle CA-1-Hessen der Hessen-PKI erhält ihr Zertifikat von der Wurzelzertifizierungsstelle und bildet damit die zweite Ebene der Zertifizierungshierarchie. Die Hessen-PKI gibt digitale Zertifikate für natürliche Personen, Gruppen und IT-Systeme aus.

Unterhalb der CA-1-Hessen werden seit 2014 keine untergeordneten CAs mehr betrieben.

1.1 Überblick

Das vorliegende Certification Practice Statement (CPS) der Hessen-PKI beschreibt die Maßnahmen der Hessen-PKI, um den Anforderungen der PCA-1-Verwaltung ([1] ergänzt um [2]) zu entsprechen.

Das CPS basiert auf dem RFC 3647.

Die Regelungen dieser CP gelten ausschließlich für die innerhalb der Hessen-PKI erstellten und entsprechend gekennzeichneten Zertifikate (siehe Abschnitt 7.1). Für außerhalb der Hessen-PKI erstellte Zertifikate gelten die Regelungen der jeweiligen PKI.

Die Hessen-PKI erstellt für folgende Zertifikatsnehmer:

- Für natürliche Personen und Gruppen von natürlichen Personen werden Zertifikate für die S/MIME Verschlüsselung und S/MIME Signatur erstellt.
- Für IT-System und IT-Prozesse werden Zertifikate für Transport Layer Security (TLS) ausgestellt.
- Zudem erstellt die Hessen-PKI folgende, für den Betrieb der CA notwendigen Zertifikate: OCSP-Response-Signing-Zertifikate für den für die Hessen-PKI genutzten OCSP-Responder (http://ocsp.hessen.de/ocsp)

1.2 Dokumentenname und Identifikation

Das vorliegende Dokument wird als Certification Practice Statement der Hessen-PKI bezeichnet. Im Namen ist die jeweils gültige Versionsnummer enthalten. Die Versionsnummer des CPS besteht aus mindestens 2 Teilen, die durch Punkte getrennt sind:

- Freigabenummer (NN)
- Bearbeitungsnummer (BB)

1.3 PKI Teilnehmer

Teilnehmer der Hessen-PKI sind Mitarbeiter des Landes Hessen bzw. seiner Verwaltungseinheiten oder Institutionen, Gruppen von Mitarbeitern sowie IT-Systeme und IT-Prozesse, die im Auftrag des Landes Hessen betrieben werden.

1.3.1 Zertifizierungsstellen

Die Zertifizierungsstellen der Hessen-PKI werden als direkte untergeordnete Zertifizierungsstellen (Sub-CA) der V-PKI betriebenen und stellen Zertifikate für Benutzer, Benutzergruppen (für die gemeinsame Verwendung von Postfächer) und IT-Systeme sowie IT-Prozesse aus.

1.3.2 Registrierungsstellen

Die Registrierungsstellen sind verantwortlich für die Prüfung der Identität von Benutzern und den organisatorischen Ablauf der Beantragung von Zertifikaten. Die Zentrale Registrierungsstelle kann diese Prozesse an geschulte PKI-Rollenträger der jeweiligen Verwaltungseinheit oder Institution des Landes Hessen abtreten.

1.3.3 Zertifikatsnehmer

Zertifikatsnehmer sind:

- IT-Systeme, die durch das Land bzw. dessen Dienststellen oder im Auftrag des Landes bzw. dessen Dienststellen betrieben werden,
- IT-Prozesse, die durch das Land bzw. dessen Dienststellen oder im Auftrag des Landes bzw. dessen Dienststellen betrieben werden,
- Natürliche Personen (Mitarbeiter des Landes Hessen bzw. dessen Dienststellen, externen Dienstleister des Landes oder dessen Dienststellen, Mitarbeiter von im Auftrag des Landes Hessen oder dessen Dienststellen tätiger Unternehmen, externe Mitarbeiter des Landes Hessen oder dessen Dienststellen in der Beschäftigungsform Arbeitsnehmerüberlassung) oder

- Gruppen von natürlichen Personen (diese setzen sich aus den unter natürliche Personen gelisteten Personengruppen zusammen).

Die Zertifikate für Zertifikatsnehmer werden von den Zertifizierungsstellen (Sub-CAs) der Hessen-PKI ausgestellt.

1.3.4 Zertifikatsnutzer

Zertifikatsnutzer der System-PKI sind alle Personen, Organisationen (die Definition einer Organisation im Sinne dieser CPS findet sich in Abschnitt 1.3.5) oder IT-Systeme, die im Rahmen der IT-Nutzung Zertifikate der Hessen-PKI verwenden oder Zugriff auf IT-Systeme des Landes Hessen haben, die ihre Dienste unter Nutzung von Zertifikaten der Hessen-PKI bereitstellen.

1.3.5 Andere Teilnehmer und PKI-Rollen

Innerhalb dieses Certification Practice Statements werden sämtliche Drittorganisationen, die nicht Teil der Verwaltung des Landes Hessen sind als Organisation bezeichnet. Hierbei kann es sich sowohl um juristische Personen, Körperschaften und Organisationen der öffentlichen Verwaltung handeln.

Innerhalb der Hessen-PKI existieren zudem die folgenden definierte PKI-Rollen und Teilnehmer:

- Schlüsselverantwortlicher
  Wenn es sich bei dem Zertifikatsnehmer um eine Benutzergruppe oder ein IT-System handelt, ist die Benennung eines Schlüsselverantwortlichen vorgeschrieben, der Sorge trägt, dass von allen Gruppenzertifikatsteilnehmern den Teilnahmebedingungen entsprochen wird.
- Gruppenzertifikatsteilnehmer
  Person mit Zugriff auf ein Gruppenpostfach mit zugeordnetem Gruppenzertifikaten oder eines IT-Systems bzw. IT-Prozesses.
- PKI-Verantwortlicher
  Der PKI-Personalverantwortliche übernimmt als Mitarbeiter einer Verwaltungseinheit oder Institution des Landes Hessens die Identitätsprüfung von natürlichen Personen, die Zertifikate der Hessen-PKI erhalten oder PKI-Rollen wahrnehmen, und organisiert die Beantragung von Zertifikaten für Mitarbeiter von Verwaltungseinheiten und Institutionen des Landes Hessen.

1.4 Verwendung von Zertifikaten

1.4.1 Zulässige Verwendung von Zertifikaten

Zertifikate der Hessen-PKI werden für die Gewährleistung der folgenden Schutzziele durch die in Abschnitt 1.3.3 genannten Zertifikatsnehmer verwendet:

o Vertraulichkeit:
  Die Daten sollen nur für die Personen nutzbar sein, die dazu autorisiert sind. Die Vertraulichkeit wird durch Verschlüsselung von Daten gewährleistet, so dass die Daten nur durch den Absender und den bzw. die Empfänger der Daten im Klartext lesbar sind.

- Integrität:
  Kryptografische Verfahren gewährleisten, dass Informationen nicht unbemerkt verändert werden können. Die Integrität wird durch die digitale Signatur von Daten bzw. Dateien gewährleistet. Dies garantiert, dass Änderungen an den Daten bzw. der Datei nach Durchführung der Signatur im Rahmen der Signaturprüfung erkannt werden.
- Authentizität:
  Authentizität gewährleistet, dass die Informationen auch tatsächlich vom betreffenden Absender stammen. Die Authentizität wird auch als Ursprungsnachweis bezeichnet und wird ebenfalls über die digitale Signatur gewährleistet. Durch diese wird eine Datei oder Authentifizierung eindeutig einer erstellenden Entität zugeordnet.

Der Verwendungszweck von Zertifikaten MUSS in der KeyUsage oder der Extended KeyUsage der jeweiligen Zertifikate hinterlegt sein.

Zertifikate dürfen nur für den im Zertifikat hinterlegten Zweck verwendet werden.

Die Zertifikate dürfen ausschließlich für dienstliche Zwecke genutzt werden.

1.4.2 Nicht zulässige Verwendung von Zertifikaten

Eine Nutzung der von der Hessen-PKI ausgestellten Zertifikate für die qualifizierte elektronische Signatur nach deutschem Signaturgesetz (SigG) bzw. electronic IDentification, Authentication and trust Services (eIDAS) ist nicht zulässig.

Eine Nutzung der von der Hessen-PKI ausgestellten Zertifikate für IT-System oder IT-Prozesse für die fortgeschritten Signatur nach deutschem Signaturgesetz (SigG) bzw. electronic IDentification, Authentication and trust Services (eIDAS) ist nicht zulässig.

Eine Nutzung der Zertifikate für andere Zwecke als den im Zertifikat hinterlegten Zweck ist nicht zulässig. Eine Nutzung der von der Hessen-PKI ausgestellten Zertifikate für die Qualifizierte elektronische Signatur nach SigG ist nicht vorgesehen.

1.5 Pflege der Richtlinie

1.5.1 Zuständigkeit für das Dokument

Verantwortlich für die Erstellung und Pflege des Dokumentes ist die Hessen-PKI, HZD. Die Richtlinie wird bei Bedarf geändert, die Regelungen für Änderungen sind in 9.12 dokumentiert.

1.5.2 Ansprechpartner

Die Pflege der vorliegenden Richtlinie erfolgt durch:

Betreiber:	Hessische Zentrale für Datenverarbeitung (HZD)
	Mainzer Straße 29
	61585 Wiesbaden
Zuständige Stelle:	Hessen-PKI, P6

Telefon:	+49 611 340 1881
Fax:	+49 611 32763 1881
E-Mail:	pki@hzd.hessen.de
Webseite:	http://pki.hessen.de

1.5.3 Eignungsprüfung für Regelungen für den Zertifizierungsbetrieb (CPS) gemäß Zertifizierungsrichtlinie

Die Eignungsprüfung wird durch den Ansprechpartner (siehe 1.5.2) durchgeführt.

1.5.4 Verfahren zur Anerkennung von Regelungen für den Zertifizierungsbetrieb (CPS)

Siehe Abschnitt 1.5.3.

1.6 Definitionen und Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority, Zertifizierungsstelle
CP	Certificate Policy
CPS	Certification Practice Statement, Beschreibung der technischen Umsetzung der Anforderungen der PKI-Policy
HZD	Hessische Zentrale für Datenverarbeitung
OCSP	Online Certificate Status Protocol, Internet-Protokoll zur Prüfung von Zertifikaten
PCA	Policy CA der Verwaltung-PKI, Wurzelzertifizierungsstelle der Verwaltungs-PKI
PCA-1-Verwaltung	Policy CA der Verwaltungs-PKI, Wurzelzertifizierungsstelle der Verwaltungs-PKI
PKI	Public Key Infrastruktur
RFC	Request for Comments
SigG	Deutsches Signaturgesetz
VDV	Verzeichnisdienst der Verwaltung (X.500-Verzeichnis des IVBB)
V-PKI	PKI der Verwaltung
ZRA	Zentrale Registrierungsstelle

2 Verantwortlichkeiten für Veröffentlichung und Verzeichnisse

2.1 Verzeichnisse

Die Bereitstellung der in 2.2 und 2.3 genannten Zertifikatsinformationen erfolgt im Internet und im internen Netz des Landes Hessen auf hochverfügbaren Verzeichnissen. Die internen Bereitstellungspunkte sind nicht über das Internet erreichbar.

Als Verzeichnisse für die Bereitstellung von Zertifikatsinformationen im Internet werden der Verzeichnisdienst der Bundesverwaltung (ldap://x500.bund.de und http://x500.bund.de) und ein vom Land Hessen betriebenes Web-Portal (http://pki.hessen.de) verwendet.

Im internen Netz werden Zertifikatsinformationen in verschiedenen Verzeichnisdiensten sowie einem internen Web-Portal bereitgestellt.

2.2 Veröffentlichung von Informationen über die Zertifikatserstellung

Die Veröffentlichung von Zertifikatsinformationen hängt von dem Bereitstellungspunkt ab. Teilnehmerzertifikate und Unterlagen für die Zertifikatsbeantragung werden durch die Hessen-PKI ausschließlich im internen Netz bereitgestellt.

Folgende Zertifikatsinformationen werden sowohl im Internet als auch im internen Netz bereitgestellt.

- Sperrinformationen zu Teilnehmer-Zertifikaten
- Zertifikat der CA-1-Hessen*NN*
- Kontaktinformationen zur Hessen-PKI

2.3 Zeitpunkt und Häufigkeit der Veröffentlichung

Im Rahmen der Hessen-PKI erfolgt die Veröffentlichung wie folgt:

- Sperrlisten werden nach Erzeugung sowohl im internen Netz als auch im Internet publiziert.
- Zertifikate werden zeitnah (in der Regel am gleichen Tag) publiziert.
- Sonstige Informationen werden zeitnah nach Änderung publiziert.

2.4 Zugriffschutz für Verzeichnisse

Der Zugriff auf die in 2.2 genannten, sowohl im Internet als auch im internen Netz bereitgestellten Informationen ist ohne Authentifizierung möglich.

Die Bereitstellung von Teilnehmerzertifikate durch die Hessen-PKI erfolgt in Verzeichnissen, auf die nur Mitarbeiter der Landes Hessens zugreifen können.

3 Identifizierung und Authentifizierung

3.1 Namen

3.1.1 Namenformen

Der Zertifikatsnehmer (Antragsteller) wird grundsätzlich im Zertifikat als eindeutigen Namen (DN) nach X.500 im folgenden Schema eingetragen:

CN=<Eindeutiger Name>
OU=<Dienststellenabkürzung>
O=Land Hessen
C=DE

Folgende Angaben sind zusätzlich zulässig:

- In Zertifikaten für natürliche Personen und Benutzergruppen (für die gemeinsame Verwendung von Postfächer) ist zusätzlich das Attribut E=<E-Mail-Adresse> im DN und im subjectAlternativeName enthalten.
- Bei Benutzergruppen (für die gemeinsame Verwendung von Postfächer) muss der CN mit der Zeichenfolge "GRP: " beginnen. Anschließend ist durch ein Leerzeichen getrennt der eindeutige Gruppennamen eingetragen (Beispiel: CN=GRP: Hessen-PKI, ...)
- In Zertifikaten für IT-Systeme und IT-Prozessen können optional die Attribute L=<Ort> und ST=<Bundesland> enthalten sein. Zertifikate für IT-System dürfen sowohl im DN als auch im subjectAlternativeName keine E-Mail-Adresse enthalten.

Bei Zertifikaten für IT-Systeme kann zusätzlich die Erweiterung subjectAlternative-Name verwendet werden, um mehrere DNS-Namen einzutragen.

Bei ausschließlich intern verwendeten Zertifikaten sind Abweichungen von der Namensregel möglich, wenn dies technisch notwendig ist.

3.1.2 Aussagefähigkeit von Namen

Die Aussagefähigkeit der Namen ist durch die Struktur des Distinguished Names gewährleistet.

Für die Schreibweise von Umlauten ist folgende Konvention verbindlich:

- Ä / ä wird ersetzt durch Ae / ae
- Ö / ö wird ersetzt durch Oe / oe
- Ü / ü wird ersetzt durch Ue / ue
- ß wird ersetzt durch ss

3.1.2.1 Zertifikat für CA-1-Hessen

Der X.500 Subject-DN der CA-1-Hessen wird wie folgt gebildet:

Attribut (X.520)	**Inhalt**
CommonName (CN)	CA-1-Hessen[xx] [xx] ist die laufende Nummer der CA, beginnend bei „01“. („00“ für den Pilotbetrieb)
OrganisationalUnit (OU)	Land Hessen
Organisation (O)	PKI-1-Verwaltung
Country (C)	DE

Der X.500 Subject-DN einer der CA-1-Hessen untergeordneten Zertifizierungsstelle, enthält im Namen vor der laufenden Nummer die Abkürzung der betreibenden Dienststelle. Ab der CA-1-Hessen04 wird keine Sub-CA mehr betrieben.

3.1.2.2 Zertifikate für natürliche Benutzer

Der X.500 Subject-DN für einen Zertifikatsinhaber der Hessen-PKI wird nach folgender Regel gebildet:

Attribut (X.520)	**Inhalt**
E-Mail (E)	E-Mail-Adresse des Zertifikatsinhabers. Da die E-Mail-Adresse im Land Hessen eindeutig ist, wird hierüber die Eindeutigkeit des Subject-DN sichergestellt.
CommonName (CN)	Natürlicher Name des Zertifikatsinhabers in der Form: Nachname Vorname[n] [Titel] [Initialen/Nr.].
OrganisationalUnit (OU)	Die Organisationseinheit wird entsprechend den Regeln des HMdIuS über die "Bezeichnung der Ministerien und nachgeordneten Behörden: Amtliches Verzeichnis hessischer Verwaltungsvorschriften – Gültigkeitsverzeichnis" festgelegt.
Organisation (O)	Land Hessen
Country (C)	DE

3.1.2.3 Gruppenzertifikate

Der X.500 Subject-DN für ein Gruppenpostfach wird nach folgender Regel gebildet.

Attribut (X.520)	**Inhalt**
E-Mail (E)	E-Mail-Adresse des Gruppenpostfaches. Da die E-Mail-Adresse im Land Hessen eindeutig ist, wird hierüber die Eindeutigkeit des Subject-DN sichergestellt.
CommonName (CN)	Bezeichnung der Funktion des Postfaches bzw. der Gruppenbezeichnung. Die verwendeten Gruppennamen sind eindeutig, die zusätzlich eingefügte Zeichenfolge "GRP: " gewährleistet die Identifizierbarkeit von Gruppenzertifikaten. Der Name wird ohne Leerzeichen geschrieben, Bindestriche sind erlaubt
OrganisationalUnit (OU)	Die Organisationseinheit wird entsprechend den Regeln des HMdIuS über die Bezeichnung der Ministerien und nachgeordneten Behörden: Amtliches Verzeichnis hessischer Verwaltungsvorschriften – Gültigkeitsverzeichnis – festgelegt.
Organisation (O)	Land Hessen
Country (C)	DE

3.1.2.4 IT-Systeme und IT-Prozesse

Der X.500 Subject-DN für ein Zertifikat für ein IT-System bzw. einen IT-Prozess wird nach folgender Regel gebildet:

Attribut (X.520)	**Inhalt**
CommonName (CN)	DNS-Name des SSL-Servers
OrganisationalUnit (OU)	Betreiber des SSL-Servers Die Organisationseinheit wird entsprechend den Regeln des HMdIuS über die Bezeichnung der Ministerien und nachgeordneten Behörden: Amtliches Verzeichnis hessischer Verwaltungsvorschriften – Gültigkeitsverzeichnis – festgelegt.
Organisation (O)	Land Hessen
Country (C)	DE

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsnehmer

Pseudonyme und anonyme Zertifikate sind in der Hessen-PKI nicht zugelassen.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Für die Attribute des Distinguished Names und des Subjects sind folgende Zeichen zulässig.

Zulässige Werte für Distinguished Names

Attribut	**Zulässige Werte**
CN einer natürlichen Person	A-Z, a-z, 0-9, "-", Leerzeichen
CN einer Gruppe	A-Z, a-z, 0-9, "-"
CN eines IT-Service	A-Z, a-z, 0-9, "-", Punkt
OU	A-Z, a-z, 0-9, "-"
E	A-Z, a-z, 0-9, "-", "@", Punkt
L	A-Z, a-z, 0-9, "-", Leerzeichen, Punkt

Feste Werte für Distinguished Names

Attribut	**Feste Werte**
O	Land Hessen
C	DE
ST	Hessen

Zulässige Werte für SubjectAlternativeName

Attribut	**Zulässige Werte**
CN einer natürlichen Person	A-Z, a-z, 0-9, "-", "@", Punkt
CN einer Gruppe	A-Z, a-z, 0-9, "-", "@", Punkt
CN eines IT-Service	A-Z, a-z, 0-9, "-", Punkt

3.1.5 Eindeutigkeit von Namen

Der von der PCA für die Hessen-PKI freigegebene Namensraum lautet „Land Hessen“, dieser ist als Organisationsbezeichnung in allen Zertifikaten der Hessen-PKI enthalten.

Bei der Erst-Registrierung wird dem Endanwender im Zertifikat ein eindeutiger Name, der so genannte Distinguished Name (DN), zugeordnet. Der Distinguished Name muss einen Teilnehmer oder eine PKI-Komponente eindeutig identifizieren. Dies ist insbesondere für den Rückschluss auf den Schlüsselinhaber bei der Nutzung von Zertifikaten und Sperrlisten notwendig. Der DN wird gemäß dem internationalen Standard X.500 gebildet.

3.1.6 Anerkennung, Authentifizierung und Funktionen von Warenzeichen

Keine Bestimmungen.

3.2 Überprüfung der Identität bei Erstantrag

3.2.1 Nachweis des Besitzes des privaten Schlüssels

Der Nachweis des Besitzes des privaten Schlüssels ist nur bei Einreichung eines Certificate Signing Request relevant, in diesem Fall ist der elektronische Request (CSR) mit dem privaten Schlüssel signiert.

Vor der Zertifizierung der öffentlichen Schlüssel der Endanwender wird durch Prüfung der Signatur des Certificate Signing Requests im PKCS#10 Format sichergestellt, dass auch die entsprechenden geheimen Schlüssel vorliegen.

Dieses Beweisverfahren gilt auch für SSL-Server- sowie CA-Zertifikate. Auch die Zertifizierungsanfrage der CA-1-Hessen an die PCA wird gemäß PKCS#10 mit dem korrespondierenden geheimen Schlüssel der CA signiert.

Bei S/MIME Zertifikaten wird der private Schlüssel durch die Registrierungsstelle erstellt.

3.2.2 Authentifizierung von Organisationen

Es werden keine Zertifikate für andere Organisationen ausgestellt.

3.2.3 Authentifizierung natürlicher Personen

Personen, die ein Endanwender-Zertifikat beantragen, werden durch ihr persönliches Erscheinen in der Registrierungsstelle oder bei dem zuständigen PKI-Verantwortlichen identifiziert und anhand eines gültigen amtlichen Lichtbildausweises authentisiert. Als amtlicher Lichtbildausweis wird der Personalausweis oder der Reisepass mit gültigem Begleitdokument, welches die Angabe zum aktuellen Wohnsitz enthält, akzeptiert. Liegt beides nicht vor, so ist der Dienstausweis bzw. ein von der Dienststelle beglaubigter Nachweis vorzulegen.

Zur Beantragung eines SSL-Server-Zertifikats und Zertifikaten für Benutzergruppen (für die gemeinsame Verwendung von Postfächer) wird zunächst durch die für den Einsatz des SSL-Servers (bzw. des Gruppenzertifikats) verantwortliche Stelle (Vollmacht gebende Stelle) ein Schlüsselverantwortlicher benannt, der für die ordnungsgemäße Verwendung des Schlüsselmaterials verantwortlich ist. Dazu erteilt die Vollmacht gebende Stelle dem Schlüsselverantwortlichen schriftlich die Berechtigung zur Wahrnehmung seiner Funktion als Schlüsselverantwortlicher eines Gruppenzertifikates und teilt dieses der Hessen-PKI mit.

Zur Beantragung eines SSL-Server-Zertifikats authentisiert sich der benannte Schlüsselverantwortliche durch persönliches Erscheinen bei der Registrierungsstelle oder bei dem zuständigen PKI-Verantwortlichen und der Vorlage seines amtlichen Lichtbildausweises. Zudem weist er seine Berechtigung als Schlüsselverantwortlicher der Registrierungsstelle anhand der von der Vollmacht gebenden Stelle ausgestellten schriftlichen Bestätigung nach. Die Namen der hierzu autorisierten Schlüsselverantwortlichen werden der zentralen Registrierungsstelle von der Hessen-PKI mitgeteilt. Den technischen Zertifizierungsantrag erhält die Registrierungsstelle im PKCS#10-Format.

3.2.4 Nicht überprüfte Teilnehmerangaben

Keine Bestimmungen.

3.2.5 Überprüfung der Berechtigung

Der Rollenträger PKI-Personalverantwortlicher der Dienststelle des Antragstellers überprüft die Angaben im Zertifikatsantrag (insbesondere Zugehörigkeit zur Institution) und bestätigt die Korrektheit der Angaben durch seine handschriftliche Unterschrift auf dem Antragsformular.

3.2.6 Gewährleistung der Zusammenarbeit

Das Certification Practice Statements sowie die Profile der innerhalb der System-PKI erstellten Zertifikate und Sperrlisten sowie der OCSP Responses entsprechen den in diesem CPS dokumentierten Standards.

3.3 Identifizierung und Authentifizierung bei Schlüsselerneuerung

3.3.1 Identifizierung und Authentifizierung bei routinemäßiger Schlüsselerneuerung

Das Verfahren entspricht einer Erstbeantragung von Zertifikaten.

3.3.2 Identifizierung und Authentifizierung bei Schlüsselerneuerung nach Sperrung

Das Verfahren entspricht einer Erstbeantragung von Zertifikaten.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Im Rahmen der Zertifikatserstellung wird natürlichen Personen und dem Schlüsselverantwortlichen von Gruppenzertifikaten ein Sperrkennwort bereitgestellt, über das eine Sperrung beantragt werden kann.

Eine Sperrung ist zudem über ein Ticket System möglich. In diesem Fall erfolgt zur Überprüfung der Identität ein Rückruf an die hinterlegte dienstliche Telefonnummer.

4 Anforderungen an Verwaltung von Zertifikats-Lebenszyklus

4.1 Zertifikatsantrag

4.1.1 Berechtigung zur Antragsstellung

Mitarbeiter des Landes können für dienstliche Zwecke Zertifikate für sich selbst, für eine Benutzergruppe (für die gemeinsame Verwendung von Postfächer) sowie für IT-Systeme bzw. IT-Prozesse beantragen.

4.1.2 Verfahren und Zuständigkeiten

Der Registrierungsprozess für Benutzer- und Benutzergruppenzertifikate basiert auf einem schriftlichen Antragsformular. Es besteht die Möglichkeit zur Verwendung von elektronischen Antraglisten in einem automatisierten Verfahren.

Im Rahmen des Registrierungsprozesses erfolgt:

- Prüfung der Identität des Antragsstellers durch die Rolle PKI-Personalverantwortlicher. Prüfung der Akzeptanz der Teilnahmepflichten an der Hessen-PKI durch den Zertifikatsnehmer bzw. Schlüsselverantwortlichen.
- Prüfung schriftliches Antragsformular
- Prüfung Antragsdaten auf Vollständigkeit und Entsprechung zu den Namensregeln.
- Bei Zertifikaten für IT-Systeme bzw. IT-Prozessen erfolgt zusätzlich eine Prüfung des elektronischen Antrags im PKCS#10-Format.

4.2 Bearbeitung des Zertifikatsantrages

4.2.1 Durchführung der Identifizierung und Authentifizierung

Siehe 3.2.3 und 3.2.5.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Nach erfolgreicher Prüfung aller notwendigen Informationen für die Zertifikatserstellung sowie Authentifizierung des Zertifikatsnehmers bzw. Schlüsselverantwortlichen wird ein Zertifikatsantrag angenommen, ansonsten erfolgt eine Ablehnung.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Die Bearbeitung richtet sich nach den organisatorischen und technischen Gegebenheiten, Registrierungsstellen können Termine für die Bearbeitung von Zertifikatsanträgen festlegen.

Der rechtzeitige Eingang von Zertifikatsanträgen ist Voraussetzung für die Zertifikatsgenerierung an definierten Terminen.

Es besteht kein Anspruch auf eine sofortige Bearbeitung von Zertifikatsanträgen.

4.3 Zertifikatsausgabe

4.3.1 Aktionen des Zertifizierungsdiensteanbieters bei der Ausgabe von Zertifikaten

4.3.1.1 Benutzer- und Gruppenzertifikate

Nach Annahme von Zertifikatsanträgen (siehe 4.2.1 und 4.2.2) erfasst der Registrierungsmitarbeiter die für das Zertifikat relevanten Daten des Antragstellers digital und erstellt eine Zertifizierungsanforderung im PKCS#10 Format.

Die von der CA erzeugten Endanwender-Zertifikate werden anschließend zusammen mit dem zugehörigen privaten Schlüssel exportiert und durch ein Transport-Kennwort geschützt im PKCS#12 gespeichert und dem Zertifikatsnehmer bzw. Schlüsselverantwortlichen in digitaler Form bereitgestellt.

Parallel erfolgt der Ausdruck eines Kennwort-Briefes mit Transport- und Sperrkennwort, das in einem verschlossenen Briefumschlag - in der Regel per Dienstpost - an den Zertifikatsnehmer bzw. den Schlüsselverantwortlichen übersandt wird.

Der Prozess der Erstellung kann in einem automatisierten Verfahren stattfinden.

4.3.1.2 Zertifikate für IT-Systeme und IT-Prozesse

Nach erfolgreicher Prüfung des Zertifikatsantrags (siehe 4.2.1 und 4.2.2) sowie der Zertifizierungsanforderung im PKCS#10 Format erfolgt die Erstellung durch die CA. Die erzeugten Zertifikate werden dem Schlüsselverantwortlichen in digitaler Form bereitgestellt.

4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats durch die CA

Im Rahmen der Ausstellung von S/MIME -Zertifikaten erfolgt eine automatische E-Mail-Benachrichtigung an die im Zertifikat enthaltene E-Mail Adresse des Zertifikatsnehmers.

4.4 Zertifikatsannahme

4.4.1 Verhalten für eine Zertifikatsannahme

Der Zertifikatsnehmer bzw. der Schlüsselverantwortliche muss einer Zertifikatsannahme innerhalb von 14 Tagen widersprechen.

4.4.2 Veröffentlichung des Zertifikats durch die CA

Zertifikate für die S/MIME Verschlüsselung werden intern in Verzeichnissen veröffentlicht.

Eine externe Veröffentlichung von Zertifikaten durch den Zertifizierungsdiensteanbieters ist nicht vorgesehen.

4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats

Eine Benachrichtigung findet nicht statt.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Zertifikate und private Schlüssel dürfen nur gemäß der vom Zertifikatsnehmer bzw. den Teilnehmer von Gruppenzertifikaten persönlich unterschriebenen Teilnahmebedingungen gespeichert und genutzt werden.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Keine Vorgaben

4.6 Zertifikatserneuerung

Eine Zertifikatserneuerung (Wiederverwendung von bereits für ein anderes Zertifikat verwendetes Schlüsselmaterial) ist nicht zulässig. Es wird bei Bedarf neues Schlüsselmaterial erzeugt. Das Verfahren entspricht einem Erstantrag (siehe 4.1).

4.6.1 Bedingungen für eine Zertifikatserneuerung

Siehe 4.6.

4.6.2 Wer darf eine Zertifikatserneuerung beantragen?

Siehe 4.6.

4.6.3 Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung

Siehe 4.6.

4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Siehe 4.6.

4.6.5 Verhalten für die Annahme einer Zertifikatserneuerung

Siehe 4.6.

4.6.6 Veröffentlichung der Zertifikatserneuerung durch die CA

Siehe 4.6.

4.6.7 Benachrichtigung anderer PKI-Teilnehmer über die Erneuerung des Zertifikats

Siehe 4.6.

4.7 Zertifizierung nach Schlüsselerneuerung

4.7.1 Bedingungen für eine Zertifizierung nach Schlüsselerneuerung

Der Zertifikatsnehmer oder der Schlüsselverantwortliche soll frühestens 90 Tage vor Ablauf eines Zertifikates ein Zertifikat für den selben Verwendungszweck nach Schlüsselerneuerung beantragen.

4.7.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen?

Entspricht Erstbeantragung. Siehe 4.1.1.

4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Entspricht Erstbeantragung. Siehe 4.2.

4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Entspricht Erstbeantragung. Siehe 4.3.2.

4.7.5 Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen

Entspricht Erstbeantragung. Siehe 4.4.1.

4.7.6 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA

Zertifikate für die S/MIME Verschlüsselung ersetzen in den internen Verzeichnissen das im Rahmen der Schlüsselerneuerung ersetze und dort veröffentlichte Zertifikat.

Zur externen Veröffentlichung von Zertifikaten siehe 4.4.2.

4.7.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Entspricht Erstbeantragung. Siehe 4.4.3.

4.8 Zertifikatsänderung

Eine Zertifikatsänderung ist nicht zulässig. Es wird bei Bedarf neues Schlüsselmaterial erzeugt. Das Verfahren entspricht einem Erstantrag (siehe 4.1).

4.8.1 Bedingungen für eine Zertifikatsänderung

Siehe 4.8.

4.8.2 Wer darf eine Zertifikatsänderung beantragen?

Siehe 4.8.

4.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung

Siehe 4.8.

4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Siehe 4.8.

4.8.5 Verhalten für die Annahme einer Zertifikatsänderung

Siehe 4.8.

4.8.6 Veröffentlichung der Zertifikatsänderung durch die CA

Siehe 4.8.

4.8.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines neuen Zertifikats

Siehe 4.8.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Bedingungen für eine Sperrung

Eine Sperrung ist in folgenden Fällen notwendig:

- Ausscheiden des Zertifikatsnehmers (natürliche Person).
- Bei Verlust eines Datenträgers mit privaten Schlüsselmaterial oder Bekanntwerden einer Kompromittierung werden sämtliche betroffene Zertifikate gesperrt.
- Verlust des Kennwort-Briefes während des Transports.

- Verlust des Kennwort-Briefes nach Empfang durch Zertifikatsnehmer bzw. Schlüsselverantwortlichen.
- Auch bei einer Zertifikatssperrung aus anderen Gründen (z.B. Namensänderung) werden alle Zertifikate des Benutzers gesperrt.
- Zugriff auf Schlüsselmaterial durch unberechtigte Dritte.

Bei der Sperrung eines Zertifikats ist immer ein gültiger Sperrgrund anzugeben.

Zur Sperrung eines Benutzer- oder Maschinen-Zertifikats ist die Angabe einer der folgenden Sperrgründe erforderlich:

Sperrgrund	**Beschreibung / Beispiel**
Schlüsselkompromittierung	Der zum Zertifikat gehörende private Schlüssel wurde kompromittiert oder das Schlüsselmaterial ist nicht mehr unter alleiniger Kontrolle des Zertifikatsnehmers bzw. bei Gruppenzertifikaten oder Zertifikaten für IT-Systemen unter der Kontrolle der Gruppe, die Zertifikate nutzen soll.
Stellenkompromittierung	Der zum Zertifikat der Aussteller-CA gehörende private Schlüssel wurde kompromittiert.
Zuordnung geändert	Die im Zertifikat enthaltenen identifizierenden Daten des Zertifikatsinhabers haben sich geändert (z.B. Namensänderung) oder der Zertifikatsinhaber scheidet aus der Landesverwaltung aus. Der Server, für den ein SSL-Server-Zertifikat ausgestellt wurde, wird außer Betrieb genommen, oder ändert seinen Namen oder Verwendungszweck.
Abgelöst	Das Zertifikat wurde durch ein neues Zertifikat ersetzt (z.B. bei defekter Smartcard).

4.9.2 Wer kann eine Sperrung beantragen?

Die Sperrung kann entweder durch den Zertifikatsnehmer bzw. den Schlüsselverantwortlichen (bei Zertifikaten für Benutzergruppen oder IT-Systemen) oder durch PKI-Rollenträger (PKI-Verantwortliche) beantragt werden.

4.9.3 Verfahren für einen Sperrantrag

Die Durchführung der Sperrung geschieht nach Prüfung der Sperrberechtigung beispielsweise durch ein Sperrkennwort oder ein Ticket im Incident Management System.

4.9.4 Fristen für einen Sperrantrag

Sollten Gründe eintreten, die eine Sperrung notwendig machen, ist unverzüglich die Sperrung des entsprechenden Zertifikats zu beantragen.

4.9.5 Fristen/Zeitspanne für die Bearbeitung des Sperrantrags durch den Zertifizierungdiensteanbieter

Die Durchführung der Sperrung geschieht nach Prüfung der Sperrberechtigung unverzüglich innerhalb der regulären Geschäftszeiten.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Die Sperrinformationen sind in der Regel 24x7 abrufbar.

4.9.7 Frequenz der Veröffentlichung von Sperrlisten

Die Zertifizierungsstellen der Hessen-PKI stellen mindestens wöchentlich eine neue Sperrliste aus. Darüber hinaus wird nach der Sperrung eines Zertifikats unmittelbar eine neue Sperrliste ausgestellt. Aus organisatorischen Gründen, z.B. bei aufeinanderfolgenden Feiertagen kann die Gültigkeitsdauer einer Sperrliste erhöht werden.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die Sperrlisten werden nach Erzeugung in den internen Verzeichnissen unmittelbar publiziert.

Extern spätestens entsprechend 4.9.7.

4.9.9 Verfügbarkeit von Online-Sperrinformationen

Online-Sperrinformationen sind in der Regel 24x7 verfügbar.

4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen

Die in der System-PKI verwendeten Sperrlisten entsprechen dem Standard X.509 v2 (vgl. RFC 5280).

Für OCSP siehe Abschnitt 4.10.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Keine Vorgaben.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Bei Verdacht einer Kompromittierung eines geheimen Schlüssels oder eines Datenträgers auf dem der private Schlüssel gespeichert ist, ist unverzüglich die Sperrung des entsprechenden Zertifikats zu beantragen.

4.9.13 Bedingungen für eine Suspendierung

Eine Suspendierung, d.h. zeitweise Sperrung eines Zertifikats, erfolgt nicht.

4.9.14 Wer kann eine Suspendierung beantragen?

Siehe 4.9.13.

4.9.15 Verfahren für Anträge auf Suspendierung

Siehe 4.9.13.

4.9.16 Begrenzungen für die Dauer von Suspendierungen

Siehe 4.9.13.

4.10 Statusabfragedienst für Zertifikate (OCSP)

Von der System-PKI wird OCSP bereitgestellt um den Sperrstatus von Teilnehmer-Zertifikaten zu prüfen.

Der OCSP Responder ist in der Regel 24x7 abrufbar.

4.10.1 Funktionsweise des Statusabfragedienstes

Das innerhalb der System-PKI verwendete Profil für OCSP entspricht dem RFC 5019.

4.10.2 Verfügbarkeit des Statusabfragedienstes

Keine Bestimmungen.

4.10.3 Optionale Leistungen

Keine Bestimmungen.

4.11 Beendigung des Vertragsverhältnisses

Beim Ausscheiden eines Zertifikatsinhabers werden dessen Zertifikate gesperrt.

4.12 Schlüsselhinterlegung und Wiederherstellung

4.12.1 Richtlinien und Praktiken der Schlüsselhinterlegung und –wiederherstellung

Innerhalb der Hessen-PKI soll Schlüsselmaterial immer unter alleiniger Kontrolle des jeweiligen Zertifikatsnehmers sein. Es gelten folgende Regelungen:

- Zertifizierungsstellen:
  Eine Schlüsselhinterlegung des Schlüsselmaterials von Zertifizierungsstellen findet nicht statt.
- Zertifikatsnehmer:
  Für die Schlüsselhinterlegung und –wiederherstellung gelten folgende Bedingungen:

- Durch die Hessen-PKI wird ein spezielles Backup der privaten Verschlüsselungsschlüssel der Endanwender vorgehalten.
- Das hinterlegte Schlüsselmaterial ist durch ein anerkanntes kryptografisches Verfahren gesichert.
- Die Schlüsselhinterlegung erfolgt in der ausstellenden CA.
- Die Prozesse für einen Wiederherstellung auf Schlüsselmaterial erzwingen ein 4-Augen-Prinzip.
- Das Backup wird mindestens bis Ende der Betriebszeit der jeweiligen zertifikatsausstellenden CA vorgehalten.
- Die Beauftragung der Wiederstellung ist grundsätzlich durch den Zertifikatsnehmer möglich.
  In begründeten Fällen kann die Wiederherstellung durch die Dienststelle beantragt werden. Die Hessen-PKI kann bei Zweifeln an dem berechtigten Interesse zur Wiederherstellung die Bearbeitung bis zur endgültigen juristischen Prüfung zurückzustellen.

4.12.2 Richtlinien und Praktiken zum Schutz von Sitzungsschlüsseln und deren Wiederherstellung

Eine Schlüsselhinterlegung von Sitzungsschlüsseln darf nicht stattfinden.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Jede nachgeordnete Zertifizierungsstelle des Landes Hessen wird in einem Rechenzentrum betrieben, das den Sicherheitsanforderungen des IT-Grundschutzes gemäß Bundesamt für die Sicherheit in der Informationstechnik (BSI) [2] an die Infrastruktur entspricht. Diese Sicherheitsmaßnahmen (Firewall, Härtung, Netztrennung) sind für jede Zertifizierungsstelle der PKI des Landes Hessen verbindlich und werden bei Bedarf entsprechend dem jeweiligen Stand der Technik weiterentwickelt.

Diese infrastrukturellen Sicherheitsmaßnahmen gewährleisten ein sehr hohes Sicherheitsniveau für alle in diesem Abschnitt betrachteten Aspekte.

5.1.1 Einsatzort und Gebäude

Siehe 5.1.

5.1.2 Räumlicher Zugang

Siehe 5.1.

5.1.3 Stromversorgung und Klimaanlage

Siehe 5.1.

5.1.4 Gefährdung durch Wasser

Siehe 5.1.

5.1.5 Brandschutz

Siehe 5.1.

5.1.6 Aufbewahrung von Datenträgern

Siehe 5.1.

5.1.7 Müllbeseitigung

Siehe 5.1.

5.1.8 Externe Datensicherung

Siehe 5.1.

5.2 Organisatorische Sicherheitsmaßnahmen

Jede Zertifizierungsstelle des Landes Hessen wird in einem Rechenzentrum betrieben, das sich an den Sicherheitsanforderungen des IT-Grundschutzes gemäß BSI [3] zur organisatorischen Sicherheit entspricht. Diese Sicherheitsanforderungen sind für jede Zertifizierungsstelle der PKI des Landes Hessen verbindlich.

5.2.1 Rollenkonzept

Jede Zertifizierungsstelle des Landes Hessen wird in einem Rechenzentrum betrieben, das sich an den Sicherheitsanforderungen des IT-Grundschutzes gemäß BSI [3] orientiert. Daraus ergeben sich die Anforderungen an die Rollen, die in einem Rollenkonzept dargelegt sind.

5.2.2 Mehraugenprinzip

Siehe 5.2.1.

5.2.3 Identifizierung und Authentifizierung jeder Rolle

Siehe 5.2.1.

5.2.4 Rollentrennung

Siehe 5.2.1.

5.3 Personelle Sicherheitsmaßnahmen

Jede Zertifizierungsstelle des Landes Hessen wird in einem Rechenzentrum betrieben, das mindestens die Sicherheitsanforderungen des IT-Grundschutzes gemäß BSI [3] an das Personal erfüllt. Diese Sicherheitsanforderungen sind für jede Zertifizierungsstelle der PKI des Landes Hessen verbindlich.

Die Hessen-PKI gewährleistet, dass Rollenträger über die notwendigen Kenntnisse und Dokumentationen für die zugeordneten Aufgaben verfügen.

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit der Mitarbeiter

Siehe 5.3.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Siehe 5.3.

5.3.3 Anforderungen an Schulungen

Siehe 5.3.

5.3.4 Häufigkeit von Schulungen und Belehrungen

Siehe 5.3.

5.3.5 Häufigkeit und Folge von Job-Rotation

Siehe 5.3.

5.3.6 Maßnahmen bei unerlaubten Handlungen

Siehe 5.3.

5.3.7 Anforderungen an freie Mitarbeiter

Siehe 5.3.

5.3.8 Dokumente, die dem Personal zur Verfügung gestellt werden müssen

Siehe 5.3.

5.4 Überwachungsmaßnahmen

5.4.1 Überwachte Ereignisse

Innerhalb der Hessen-PKI werden folgende Ereignissen überwacht:

- Ereignisprotokollen und Logs auf PKI-Systemen
  - Konfigurationsänderung oder Manipulation der vorgesehenen Konfiguration
  - Erschleichung von Zertifikaten
  - Nicht vorgesehene Ereignisse oder System-Zustände
  - Veränderung der Gruppenmitgliedschaften der Rollenträger der Zertifizierungsstelle.
  - Auftretende Fehler
- Plausibilität der Zertifikatsanfragen
- Einhaltung der Prozesse zur Registrierung von Zertifikaten

5.4.2 Häufigkeit der Protokollanalyse

Die Überwachung von Ereignisprotokollen und Logs auf Zertifizierungsstellen der Hessen-PKI erfolgt durch eine Security Information and Event Management Lösung, diese ist 24x7 verfügbar.

Eine Überprüfung der Ereignisse in den nachgeordneten Zertifizierungsstellen und den Registrierungsstellen in Form eines Audits erfolgt mindestens alle drei Jahre sowie in Form eines Überwachungsaudits nach TR-03145-1 und TR-03147 jährlich durch unabhängige, vom BSI anerkannte Prüfstellen.
Im Falle eines Sicherheitsvorfalls erfolgt die Überprüfung unmittelbar nach Bekanntwerden des Sicherheitsvorfalls.

5.4.3 Aufbewahrungszeit von Protokolldateien

Ereignisprotokolle und Logs der Zertifizierungsstellen der Hessen-PKI und der zugehörigen Systeme werden für mindestens 60 Tage vorgehalten werden. Sicherheitskritische Ereignisse werden anschließend in der Security Information and Event Management (SIEM)-Lösung der HZD archiviert.

5.4.4 Schutz der Protokolldateien

Zugriff auf die Ereignisprotokolle und Logs haben die PKI-Administratoren bzw. HSM-Administratoren. Die Überwachung von Ereignisprotokollen und Logs über eine SIEM-Lösung der HZD ist zulässig und erfolgt für die nachgeordneten Zertifizierungsstellen im Rahmen der PKI-Auditierung.

Ereignisprotokolle und Logs der nachgeordneten Zertifizierungsstellen sind durch die Überwachung mittels SIEM vor Manipulation geschützt.

5.4.5 Datensicherung der Protokolldateien

Protokolldateien sind Teil der regelmäßig durchgeführten Backups und werden für den in Abschnitt 5.4.3 genannten Zeitraum vorgehalten.

5.4.6 Überwachungssystem (intern / extern)

Die Überwachungssysteme werden im internen Netz der HZD bzw. des Landes Hessens betrieben. Ein Zugriff ist nur von den Quellsystemen aus möglich.

5.4.7 Benachrichtigung der Ereignisauslöser

Es ist der zuständige Bereich für IT-Sicherheit der HZD zu informieren, der gemeinsam mit der unter 1.5.2 genannten Stelle über das weitere Vorgehen berät. Die Benachrichtigung erfolgt bei den nachgeordneten Zertifizierungsstellen automatisch über die SIEM-Lösung der HZD.

5.4.8 Schwachstellenanalyse

Die Schwachstellenanalyse ist Teil der Planungen der HZD zur Gewährleistung der IT-Sicherheit und wird neben den Betreibern der System-PKI durch die zuständigen Stellen für IT-Sicherheit der HZD und des Landes Hessens gewährleistet.

5.5 Archivierung

5.5.1 Archivierte Daten

Informationen über die Beantragung und Ausstellung von Zertifikaten werden im Rahmen des Lebenszyklus-Managements der CA für die Laufzeit der CA vorgehalten.

5.5.2 Aufbewahrungsfristen für archivierte Daten

Eine Aufbewahrung von Daten ist auf die Laufzeit einer CA begrenzt.

Die Aufbewahrung von Daten zur Dokumentation der Prozesse zur Bereitstellung und Betrieb der System-PKI richtet sich nach den Dokumentationsregelungen der HZD.

5.5.3 Schutz der Archive

Die Archive sind entsprechend der in Abschnitt 5.1 genannten Sicherheitsmaßnahmen geschützt.

5.5.4 Datensicherung der Archive

Im Rahmen des Verfügbarkeitsmanagements der HZD ist die Verfügbarkeit von Archiven auf Basis der Datensicherung gewährleistet.

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

Es werden keine Zeitstempeldienste verwendet.

5.5.6 Archivierungssystem (intern / extern)

Die Archivierungssysteme werden im internen Netz der HZD bzw. des Landes Hessens betrieben. Ein Zugriff ist nur von den Quellsystemen aus möglich.

5.5.7 Verfahren für Abruf und Überprüfung archivierter Daten

Im Rahmen des Verfügbarkeitsmanagements der HZD ist die Verfügbarkeit von Archiven auf Basis der Datensicherung gewährleistet.

5.6 Schlüsselerneuerung der Zertifizierungsstelle

In der PKI des Landes Hessen sind die Schlüssel und Zertifikate für ihren Anwendungszweck nur im festgelegten Gültigkeitszeitraum (siehe 6.3.2) zu verwenden. Unter Schlüsselerneuerung wird die Ausstellung eines Folgezertifikats mit einem neuen Schlüssel verstanden.

Schlüsselerneuerung der PCA

Neue Wurzelzertifikate der PCA-1-Verwaltung werden auf Gültigkeit geprüft, indem der Fingerabdruck des Wurzelzertifikats mit dem vom BSI (z.B. im Bundesanzeiger) veröffentlichten Fingerabdruck verifiziert wird. Die gültigen PCA-Zertifikate werden automatisiert in den Domänen des Landes Hessen auf die Rechner (IT-Arbeitsplätze und Server) verteilt. Für Zertifikatsnutzer ohne Benutzerkonto im Active Directory ist der Bezug der PCA-Zertifikate über das Internet gegeben.

Schlüsselwechsel der CA-1-Hessen

Zur Durchführung eines Schlüsselwechsels der CA-1-Hessen wird in einem Hardware Security Modul (siehe 6.2) ein neues Schlüsselpaar sicher erzeugt und ein neues Zertifikat beim BSI beantragt. Die Antragstellung erfolgt im PKCS#10 Format unter Berücksichtigung der Anforderungen an die Namensvergabe (vgl. 3.1). Der elektronische Zertifikatsantrag wird dem BSI im PKCS#10 Format übergeben.

Mit einem Schlüsselwechsel der CA-1-Hessen wird eine neue Zertifizierungsstelle in Betrieb genommen. Zur Ausstellung von Zertifikaten wird nach dem Schlüsselwechsel der CA-1-Hessen nur noch der neue Schlüssel herangezogen. Der Schlüssel der bisherigen CA-1-Hessen wird nur noch zur Ausstellung von Sperrlisten verwendet. Der bisherige Schlüssel signiert Sperrlisten zu Zertifikaten, die mit dem bisherigen Schlüssel ausgestellt wurden, während der neue Schlüssel die Sperrlisten zu Zertifikaten signiert, die mit dem neuen Schlüssel ausgestellt wurden. Der bisherige CA-Schlüssel wird solange zur Ausstellung von Sperrlisten verwendet, wie es mit diesem CA-Schlüssel signierte gültige Zertifikate gibt.

5.7 Kompromittierung und Wiederherstellung

Im Rahmen eines Sicherheitskonzepts zur PKI des Landes Hessen sind insbesondere die Bedrohung und Risiken der Kompromittierung des geheimen Schlüssels, das Bekanntwerden von Schwachstellen in den verwendeten kryptographischen Verfahren und die Nichtverfügbarkeit der Sperrlisten berücksichtigt und entsprechende Maßnahmen zur Minderung des daraus entstehenden Risikos entwickelt worden.

Es existiert ein für alle Zertifizierungsstellen des Landes Hessen verbindliches Verfahren für Notfälle und Katastrophen. Bei Kompromittierung des Schlüsselmaterials einer CA, werden alle von dieser CA ausgestellten Zertifikate gesperrt, und alle von der CA-1-Hessen ausgestellten und noch gültigen Zertifikate gesperrt. Die CA durch Sperrung durch die übergeordnete Zertifizierungsstelle dauerhaft außer Betrieb genommen.

5.7.1 Vorgehensweise bei Sicherheitsvorfällen und Kompromittierungen

Siehe 5.7.

5.7.2 Betriebsmittel, Software- und/oder Datenkompromittierung

Siehe 5.7.

5.7.3 Kompromittierung des privaten Schlüssels

Siehe 5.7.

5.7.4 Wiederaufnahme des Betriebs nach einer Kompromittierung

Siehe 5.7.

5.8 Einstellung des Betriebs

Die CA-1-Hessen kann die Ausstellung von Zertifikaten mit einer Ankündigungsfrist von drei Monaten ohne Angabe von Gründen einstellen. Die Ankündigung erfolgt schriftlich gegenüber der Wurzelzertifizierungsstelle und wird im Intranet des Landes Hessen veröffentlicht. Die Beendigung der Ausstellung von Zertifikaten im Notfall oder Katastrophenfall unterliegt nicht diesen Anforderungen. Für den Fall, dass die Ausstellung der Zertifikate eingestellt wird, gewährleistet die Hessen-PKI:

- für den verbleibenden Nutzungszeitraum von noch gültigen Zertifikaten den ordnungsgemäßen Betrieb.
- den Weiterbetrieb der betroffenen Zertifizierungsstellen.

Mit Einstellung des Betriebes werden alle von der CA-1-Hessen ausgestellten und noch gültigen Zertifizierungsstellen-Zertifikate gesperrt. Nach erfolgter Ankündigung werden Zertifikate für Zertifizierungsstellen nur noch mit einer Gültigkeitsdauer bis zum Zeitpunkt des Betriebsendes ausgestellt.

Der Vorgang der Einstellung des Betriebs ist im Organisations- und Betriebshandbuch beschrieben.

Soft-PSEs werden nach der Einstellung des Betriebes der CA nicht eingezogen. Somit besteht für die Anwender die Möglichkeit, verschlüsselte Daten weiterhin entschlüsseln zu können.

6 Technische Sicherheitsmaßnahmen

Jede Zertifizierungsstelle des Landes Hessen wird in einem Rechenzentrum betrieben, das sich an den Sicherheitsanforderungen des IT-Grundschutzes gemäß BSI [3] zur organisatorischen Sicherheit entspricht. Diese Sicherheitsanforderungen sind für jede Zertifizierungsstelle der PKI des Landes Hessen verbindlich.

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

Das Schlüsselmaterial der CA wird in einem 4-Augenprinzip in einem HSM erzeugt.

Das Schlüsselmaterial für die Zertifikatsnehmer natürliche Personen und Benutzergruppen wird als Soft-PSE in der Registrierungsstelle erzeugt und nach Verarbeitung automatisch gelöscht. Die Registrierungsarbeitsplätze sind gehärtete IT-Systeme, die ausschließlich autorisierten RA-Mitarbeitern zugänglich sind. Die Festplatten der Registrierungsarbeitsplätze sind verschlüsselt und werden regelmäßig sicher bereinigt.

Schlüsselmaterial für IT-Systeme und IT-Prozesse wird durch die zuständigen Administratoren auf den entsprechenden IT-Systemen erzeugt.

6.1.2 Übermittlung privater Schlüssel an Zertifikatsnehmer

Bei Erstellung der privaten Schlüssel durch die RA erfolgt die Bereitstellung von privaten Schlüssel zusammen mit den zugehörigen Zertifikaten in Kennwort-geschützten PKCS#12 Dateien.

6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsstelle

Bei Beantragung von Zertifikaten über Certificate Signing Request erfolgt die Bereitstellung des öffentlichen Schlüssels im PKCS#10 Format enthalten.

6.1.4 Lieferung öffentlicher Schlüssel an Zertifikatsnutzer

Der öffentliche Schlüssel ist in der Kennwort-geschützten PKCS#12 Dateien enthalten.

6.1.5 Schlüssellängen

Die aktuellen Empfehlungen des BSI – „Geeignete Kryptoalgorithmen gemäß §17 (2) SigV“ – sind innerhalb der Hessen-PKI verbindlich.

6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle

Die aktuellen Empfehlungen des BSI – „Geeignete Kryptoalgorithmen gemäß §17 (2) SigV“ – sind innerhalb der PKI verbindlich.

Derzeit werden folgende Schlüssellängen verwendet:

- Zertifizierungsstellen RSA 4096 bit
- Sonstige Zertifikatsnehmer mindestens RSA 2048 bit

6.1.7 Schlüsselverwendungen

Der zulässige Verwendungszweck von Zertifikaten ist in der KeyUsage sowie der Extended KeyUsage der jeweiligen Zertifikate hinterlegt sein. Siehe auch Abschnitt Siehe 1.4.1.

6.2 Schutz privater Schlüssel und Einsatz von Kryptographischer Module

Jede Zertifizierungsstelle des Landes Hessen erzeugt ihre Signaturschlüssel in einem sicheren Hardwaremodul (Hardware Security Module, kurz HSM).

6.2.1 Standards für Kryptographische Module

Das zur Generierung und Speicherung der geheimen Signaturschlüssel von Zertifizierungsstellen eingesetzte HSM muss nach einem etablierten Standard für Sicherheitsevaluierungen geprüft und von einer anerkannten Evaluierungsstelle sicherheitsbestätigt sein. Die für Zertifizierungsstellen der Hessen-PKI eingesetzte kryptografischen Module sind mindestens sicherheitsbestätigt nach Common Criteria EAL 4+.

6.2.2 Aufteilung privater Schlüssel auf mehrere Personen (n von m)

Der Zugriff auf das Schlüsselmaterial von Zertifizierungsstellen erfolgt gemäß Rollenkonzept im 4-Augen-Prinzip.

6.2.3 Hinterlegung privater Schlüssel (Key Escrow)

Eine Hinterlegung des privaten Schlüssels einer Zertifizierungsstelle findet nicht statt.

Die Regelungen für private Schlüssel von Zertifikatsnehmer sind in Abschnitt 4.12 dokumentiert.

6.2.4 Sicherung privater Schlüssel

Für die privaten Signaturschlüssel der Zertifizierungsstellen existiert ein verschlüsseltes und sicher gelagertes Backup. Die Signaturschlüssel sind unter Einhaltung des Vier-Augen-Prinzips ausschließlich in den verwendeten Hardware Security Modulen wiederherstellbar.

6.2.5 Archivierung privater Schlüssel

Eine Archivierung des privaten Schlüssels der Zertifizierungsstellen nach Ende ihrer Nutzung ist nicht vorgesehen.

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Die privaten Signaturschlüssel der Zertifizierungsstellen können nur als verschlüsseltes Backup exportiert und in ein kyptographisches Modul des gleichen Herstellers importiert werden (siehe hierzu auch 6.2.4).

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Die privaten Schlüssel sind persistent im kryptographischen Modul gespeichert. Das Modul ist mit einem Tamper-Schutz gesichert. Ein Zugriff auf die privaten Schlüssel in kryptographischen Modulen ist nur nach Authentifizierung mittels Chipkarte möglich.

6.2.8 Aktivierung privater Schlüssel

Private Signaturschlüssel einer Zertifizierungsstelle werden im HSM nach Authentisierung der Schlüsselverantwortlichen unter Einhaltung des Vier-Augen-Prinzips durch den Einsatz von Chipkarten des HSM aktiviert.

6.2.9 Deaktivierung privater Schlüssel

Nicht mehr benötigte private Signaturschlüssel der Zertifizierungsstellen werden im HSM durch dessen sichere Löschmechanismen überschrieben. Die Backup-Datenträger der privaten Schlüssel werden zerstört.

6.2.10 Zerstörung privater Schlüssel

Nicht mehr benötigte private Signaturschlüssel der Zertifizierungsstellen werden im HSM durch dessen sichere Löschmechanismen überschrieben. Die Backup-Datenträger der privaten Schlüssel werden zerstört.

6.2.11 Beurteilung kryptographischer Module

Siehe 6.2.1.

6.3 Andere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Der öffentliche Schlüssel der CA wird mindestens bis 5 Jahre nach Ende seiner Gültigkeit archiviert.

Teilnehmerzertifikate werden in Form des Zertifikates bis zum Ende der Laufzeit der ausstellenden CA vorgehalten.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Teilnehmerzertifikate haben eine maximale Laufzeit von 3 Jahren.

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation der Aktivierungsdaten

Von der Registrierungsstelle erzeugte Schlüsselmaterial für Endteilnehmer muss vor dem Import mittels 10-stelligem komplexen Kennwort aktiviert werden.

6.4.2 Schutz der Aktivierungsdaten

Die Aktivierungsdaten werden in einem verschlossenen Kennwort-Brief, der per (Haus-)Post übersandt wird, bereitgestellt.

6.4.3 Weitere Aspekte der Aktivierungsdaten

Keine Bestimmungen.

6.5 Sicherheitsmaßnahmen für Computer

Jede Zertifizierungsstelle des Landes Hessen wird in einem Rechenzentrum betrieben, das mindestens die Sicherheitsanforderungen des IT-Grundschutzes gemäß BSI [3] an die organisatorische Sicherheit erfüllt. Diese Sicherheitsanforderungen sind für jede Zertifizierungsstelle der PKI des Landes Hessen verbindlich.

6.5.1 Spezifische Anforderungen an technische Sicherheitsmaßnahmen

Siehe 6.5.

6.5.2 Beurteilung von Computersicherheit

Siehe 6.5.

6.6 Technische Maßnahmen während des Lebenszyklus

Die existierenden Sicherheitsmaßnahmen werden jährlich geprüft und gegebenenfalls weiterentwickelt.

6.6.1 Maßnahmen der Systementwicklung

Siehe 6.6.

6.6.2 Maßnahmen im Sicherheitsmanagement

Siehe 6.6.

6.6.3 Lebenszyklus der Sicherheitsmaßnahmen

Siehe 6.6.

6.7 Sicherheitsmaßnahmen für Netze

Die Netzarchitektur des Betreibers wird regelmäßig geprüft und gegebenenfalls weiterentwickelt.

6.8 Zeitstempel

Es werden keine Zeitstempeldienste bereitgestellt.

7 Profile von Zertifikaten, Sperrlisten und OCSP

7.1 Zertifikatsprofile

Das Zertifikatsprofil der in Abschnitt 1.1 genannten Zertifikatstypen ist in Anhang A dokumentiert.

7.1.1 Versionsnummern

Zertifikate entsprechen dem Standard X.509 V3

7.1.2 Zertifikatserweiterungen

Das Zertifikatsprofil der in Abschnitt 1.1 genannten Zertifikatstypen ist in Anhang A dokumentiert.

7.1.3 Algorithmen Bezeichner (OID)

1.2.840.113549.1.1.11 sha256RSA

7.1.4 Namensformen

Siehe 3.1.

7.1.5 Namensbeschränkungen

Siehe 3.1.

7.1.6 Bezeichner für Zertifikatsrichtlinien (OID)

Kryptomodul laut CP der Verwaltungs-PKI Abschnitt 8.3.2 Punkt 2 und 3 [2]	1.3.6.1.4.1.7924.1.2.8.3
HW-Token, Schlüssel nicht auslesbar	1.3.6.1.4.1.7924.1.2.8.2
SW-Modul mit Passwort (z.B. pkcs#12)	1.3.6.1.4.1.7924.1.2.8.1

7.1.7 Nutzung der Erweiterung Richtlinienbeschränkung (Policy Constraints)

Die von der Hessen-PKI ausgestellten Zertifikaten enthalten den in Abschnitt 7.1.6 genannten Kennzeichner.

7.1.8 Syntax und Semantik von Policy Qualifiers

Siehe 7.1.6.

7.1.9 Verarbeitung von kritischen Erweiterung für Zertifizierungsrichtlinien

Keine Bestimmungen, die Richtlinie ist nicht kritisch.

7.2 Sperrlistenprofile

7.2.1 Versionsnummer(n)

Die in der Hessen-PKI ausgestellten Endanwender-Zertifikate für Signatur und Verschlüsselung genügen folgendem Zertifikatsprofil:

Es werden X.509 Zertifikate der Version 3 eingesetzt.

Feld	**Inhalt**
Signature Algorithm	sha256WithRSAEncryption
Version	Versionsnummer 1 für Version 2.
Issuer	Aufbau des Subject-DN der CA gemäß 3.1
Signature	Siehe „Signature Algorithm“
LastUpdate	Ausstellungszeitpunkt
NextUpdate	Zeitpunkt des nächsten Updates
Revoked Certificates	Seriennummern der gesperrten Zertifikate mit RevocationDate
IssuerUniqueID	Nicht enthalten

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

CRL Extension	**K**	**Kommentar**
Authority Key Identifier	N	Enthält „Issuer“ und „Serialnumber“
CRL Number	N	Sperrlistennummern
Issuing DistributionPoint	N	Dieses Feld ist nicht enthalten.

Sämtliche CRL Extensions sind nicht kritisch (non-critical).

CRL Entry Extension	**K**	**Kommentar**
Reason Code	N	Der Sperrgrund "unspecified" wird nicht verwendet. "RemoveFromCRL" wird nicht verwendet.

N: nicht-kritische (non-critical) Erweiterung

J: kritische (critical) Erweiterung

7.3 Profile des Statusabfragedienstes (OCSP)

Das innerhalb der System-PKI verwendete Profil für OCSP entspricht dem RFC 5019.

7.3.1 Versionsnummer(n)

Siehe Abschnitt 7.3.

7.3.2 OCSP Erweiterungen

Siehe Abschnitt 7.3..

8 Konformitätsprüfung

Eine Überprüfung findet regelmäßig auf Grundlage der Regelungen zur IT-Revision und dem IT-Sicherheitsmanagement des Betreibers (siehe 1.5) sowie bei Bedarf durch das BSI statt. Siehe auch Abschnitt 5.4.2.

8.1 Häufigkeit und Bedingungen für Überprüfungen

Siehe 8.

8.2 Identität/Qualifikation des Prüfers

Siehe 8.

8.3 Stellung des Prüfers zum Bewertungsgegenstand

Siehe 8.

8.4 Überprüfte Bereiche

Siehe 8.

8.5 Mängelbeseitigung

Siehe 8.

8.6 Veröffentlichung der Bewertungsergebnisse

Siehe 8.

9 Andere geschäftliche und rechtliche Angelegenheiten

Die Ausgabe von Zertifikaten ist auf Mitarbeiter und IT-Systeme bzw. IT-Prozesse des Landes Hessen begrenzt.

9.1 Gebühren

Die Gebühren richten sich nach dem gültigen Leistungsentgeldverzeichnis LEV.

9.1.1 Gebühren für Zertifikate oder Zertifikatserneuerungen

Siehe Abschnitt 9.1.

9.1.2 Gebühren für den Zugriff auf Zertifikate

Siehe Abschnitt 9.1.

9.1.3 Gebühren für Sperrungen oder Statusinformationen

Siehe Abschnitt 9.1.

9.1.4 Andere Gebühren

Etwaig notwendige Key-Recoveries sind kostenpflichtig.

9.1.5 Gebührenerstattung

Die für das Key Recovery erhobenen Gebühren werden nicht erstattet.

9.2 Finanzielle Verantwortung

Die Hessen-PKI wird durch den Betreiber im Auftrag des Landes Hessen betrieben.

9.2.1 Versicherungsdeckung

Keine Regelungen.

9.2.2 Weitere Vermögenswerte

Keine Regelungen.

9.2.3 Versicherung oder Garantiedeckung für End-Entities

Keine Regelungen.

9.3 Vertraulichkeit von Geschäftsdaten

Es gelten die Regelungen des Betreibers und des Landes Hessen für die Vertraulichkeit von Geschäftsdaten.

9.3.1 Vertraulich zu behandelnde Informationen

Siehe 9.4.

9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören

Siehe 9.4.

9.3.3 Verantwortlichkeit für den Schutz vertraulicher Informationen

Der vertrauliche Informationen verarbeitende Mitarbeiter bzw. Dienststelle des Landes Hessen ist verpflichtet den Schutz von vertraulichen Informationen nach den Vorgaben des Betreibers bzw. des Landes Hessen zu gewährleisten.

9.4 Schutz personenbezogener Daten

Es gelten die allgemeinen Datenschutz-Richtlinien.

Innerhalb der Verfahren der Hessen-PKI werden nur die für die Zertifikatserstellung notwendigen Informationen verarbeitet. Sowohl die hierbei entstehenden elektronischen Daten als auch Formulare werden als vertrauliche Daten behandelt.

9.4.1 Richtlinie zur Verarbeitung personenbezogener Daten

Siehe 9.4.

9.4.2 Vertraulich zu behandelnde Daten

Siehe 9.4.

9.4.3 Nicht vertraulich zu behandelnde Daten

Siehe 9.4.

9.4.4 Verantwortung zum Schutz personenbezogener Daten

Siehe 9.4.

9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten

Es werden ausschließlich die für die Zertifikatserstellung notwendigen Informationen verarbeitet. Informationen über die verarbeiteten Daten werden in den in Abschnitt 2.1 genannten, internen Verzeichnissen bereitgestellt.
Siehe auch 9.4.

9.4.6 Offenlegung bei gerichtlicher Anordnung oder im Rahmen gerichtlicher Beweisführung

Keine Bestimmungen.

9.4.7 Andere Umstände einer Veröffentlichung

Keine Bestimmungen.

9.5 Geistiges Eigentum

Der unter 1.5.2 genannte Betreiber ist Urheber des vorliegenden Dokuments, eine unveränderte Weitergabe an Dritte ist zulässig.

9.6 Verpflichtungen

9.6.1 Verpflichtungen der Zertifzierungsstellen

Die Hessen-PKI verpflichtet sich den Regelungen in diesem CPS zu entsprechen.

9.6.2 Verpflichtungen der Registrierungsstellen

Die Registierungsstellen der Hessen-PKI verpflichtet sich den für sie geltenden Regelungen in diesem CPS zu entsprechen.

9.6.3 Verpflichtungen der Zertifikatsnehmer

Der Teilnehmer verpflichtet sich mittels Unterschrift die für ihn geltenden Teilnahmebedingungen zur Kenntnis genommen zu haben und umzusetzen.

9.6.4 Verpflichtungen der Zertifikatsnutzer

Keine Bestimmungen.

9.6.5 Verpflichtungen sonstiger Teilnehmer

Sonstige Teilnehmer verpflichten sich bei der Übernahme von Aufgaben innerhalb des Beantragungsprozesse für Zertifikate der Hessen-PKI oder bei Nutzung von Zertifikaten der Hessen-PKI zur Einhaltung der Regelungen der für die jeweiligen Zertifikate geltenden Teilnahmebedingungen.

9.7 Haftungsausschlüsse

Eine Gewährleistung wird nicht übernommen.

9.8 Haftungsbeschränkungen

Siehe Abschnitt 9.7.

9.9 Schadensersatz

Siehe Abschnitt 9.7.

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Das CPS ist ab dem auf dem Titelblatt genannten Datum gültig.

9.10.2 Aufhebung

Das CPS verliert mit Publizierung einer neueren Version oder bei Einstellung des Betriebs der PKI seine Gültigkeit.

9.10.3 Auswirkung der Aufhebung und des Weiterbestehens

Es gilt der jeweils gültige Stand der Policy. Eine Kündigung des Betriebes der System-PKI oder nachgeordneten Zertifizierungsstellen wirkt sich nicht auf die Gültigkeit der Regelungen dieser Policy aus.

9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern

Es werden keine individuellen Absprachen mit Teilnehmern getroffen.

9.12 Änderung der Richtlinie

9.12.1 Verfahren für Änderungen

Eine Aktualisierung der Policy wird nur dann den Teilnehmern offiziell bekannt gegeben, wenn dies erforderlich ist.

Bei Änderungen wird unterschieden, ob diese die Sicherheit betreffen beziehungsweise Änderungen der Abläufe seitens der Endanwender erfordern und daher einer generellen Bekanntmachung gegenüber den Endanwendern unterliegen.

Die Anpassung und Einhaltung der Policy wird durch einen Auditor überwacht.

9.12.2 Benachrichtigungsmechanismus und –fristen

Änderungen, die keiner Bekanntmachung unterliegen

Änderungen dürfen dann ohne Bekanntmachung erfolgen, wenn diese nicht relevant für die Sicherheit sind, beziehungsweise keine Änderungen seitens der Abläufe der Endanwender (Registrierung, Prüfung von Zertifikaten, Sperrungen etc.) erfordern. Insbesondere können Korrekturen zur Typographie und Layout ohne weitere Bekanntmachung erfolgen.

Änderungen, die eine Bekanntmachung erfordern

Änderungen, die die Sicherheit oder die Abläufe der Endanwender betreffen, erfordern eine zeitnahe Bekanntmachung.

9.12.3 Bedingungen für Änderung des Richtlinienbezeichners (OID)

Die OID für dieses Dokument wird geändert werden, wenn die Änderung einer Bekanntmachung erfordert.

Zertifikate, die nach der alten Version der Policy ausgestellt wurden, werden nicht geändert (d.h. enthalten weiterhin den OID der alten Version der Policy). Die Zertifikate, welche nach der Änderung der Policy ausgestellt werden, erhalten den neuen OID der Policy.

9.13 Verfahren zur Schlichtung von Streitfällen

Siehe Abschnitt 9.16

9.14 Geltendes Recht

Der Betrieb der System-PKI unterliegt den Gesetzen der Bundesrepublik Deutschland sowie den Datenschutzgesetzen des Landes Hessens.

9.15 Einhaltung geltenden Rechts

Siehe Abschnitt 9.14

9.16 Sonstige Bestimmungen

Der Betrieb der System-PKI erfolgt entsprechend den Vorgaben des Landes Hessen und der HZD.

9.16.1 Vollständigkeit

Siehe Abschnitt 9.15.

9.16.2 Abgrenzung

Siehe Abschnitt 9.15.

9.16.3 Salvatorische Klausel

Siehe Abschnitt 9.15.

9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

Siehe Abschnitt 9.15.

9.16.5 Höhere Gewalt

Siehe Abschnitt 9.15.

9.17 Andere Bestimmungen

Keine Bestimmungen.

10 Literaturverzeichnis

1	Name: Datei	Sicherheitsleitlinie der Wurzelzertifizierungsinstanz der Verwaltung, BSI, Version 3.2 vom 09.01.2003 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/VerwaltungsPKI/pca_polv3_2_pdf.pdf?__blob=publicationFile
2	Name: Datei	Ergänzungen und Änderungen zu den „Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung“ Version 3.2 vom 09.01.2003 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/VerwaltungsPKI/Ergaenzung_pca_polv3_2_pdf.pdf?__blob=publicationFile
3	Name: Datei	IT-Grundschutzkataloge In der jeweils gültigen Version

Anhang A

Zertifikatsprofile der CA-1-Hessen

Feld	Inhalt
Version	V3
Serial Number	Seriennummer des Zertifikats (8-stellig)
Signature Algorithm	Sha256WithRSAEncryption
Signature Hash Algorithm	Sha256
Issuer	CN = PCA-1-Verwaltung-NN O = PKI-1-Verwaltung C = DE
Signature	Siehe „Signature Algorithm“
Valid from	Beginn der Gültigkeit des Zertifikats
Valid to	Ende der Gültigkeit des Zertifikats
Subject	Aufbau des Subject-DN der CA gemäß 3.1.
Public Key	RSA 2048 bit
Subject Public Key Info	RSAEncryption
Issuer Unique ID	Nicht enthalten
Subject Unique ID	Nicht enthalten

Erweiterungen	K	Inhalt
Key Usage	Y	Key Cert Sign CRL Sign
Certificate Policy	N	OID=1.3.6.1.4.1.7924.1.2.8.3 Qualifier= http://www.bsi.bund.de
Application Policy	N	Entspricht Inhalt von Key Usage
Subjekt Key Identifier	N	Enthält folgende Einträge: Key ID, Issuer, Serial Number
SubjectAltName	N	rfc822 Name=pki@hzd.hessen.de URL:http://pki.hessen.de
Basic Constraints	Y	Path Length Constraint=3
CRL Distribution Points	N	ldap://x500.bund.de/CN=PCA-1-Verwaltung-15,O=PKI-1-Verwaltung,C=DE?certificateRevocationList http://x500.bund.de/cgi-bin/show_attr?cn=PCA-1-Verwaltung-15&attr=crl

N: nicht-kritische (non-critical) Erweiterung
J: kritische (critical) Erweiterung

Zertifikatsprofile der End-Entitäten

Feld	**Inhalt**
Version	V3
Serial Number	Seriennummer des Zertifikats (38-stellig)
Signature Algorithm	Sha256WithRSAEncryption
Signature Hash Algorithm	Sha256
Issuer	Aufbau des Subject-DN der CA gemäß 3.1.
Signature	Siehe „Signature Algorithm“
Valid from	Beginn der Gültigkeit des Zertifikats
Valid to	Ende der Gültigkeit des Zertifikats
Subject	Aufbau des Subject-DN des Endanwenders gemäß 3.1.
Public Key	RSA 2048 bit
Subject Public Key Info	RSAEncryption
Issuer Unique ID	Nicht enthalten
Subject Unique ID	Nicht enthalten

Erweiterungen	**K**	**Inhalt**
Key Usage	Y	S/MIME Signatur: Digital Signature / Non Repudiation S/MIME Verschlüsselung: KeyEncipherment-KeyEncipherment TLS: Digital Signature OCSP: Digital Signature
Extended Key Usage	N	S/MIME: OID 1.3.6.1.5.5.7.3.4 TLS: OID= 1.3.6.1.5.5.7.3.1 OCSP: OID=1.3.6.1.5.5.7.3.9
Certificate Policy	N	OID=1.3.6.1.4.1.7924.1.2.8.1 Qualifier= http://pki.hessen.de
Application Policy	N	Entspricht Inhalt von Key Usage
Subjekt Key Identifier	N	Entspricht der Key ID
SubjectAltName	N	Bei S/MIME: rfc822 Name TLS: Ein oder mehrere DNS-Namen bzw. IP-Adressen OCSP: TLS: DNS-Namen des OCSP Rsponders

CRL Distribution Points	N	http://pki.hessen.de/CA-1-Hessen*NN*.crl ldap://x500.bund.de/CN=CA-1-Hessen*NN*,OU=Land Hessen,O=PKI-1-Verwaltung,C=DE?certificateRevocationList Optional können noch Einträge, die sich auf interne Verzeichnisdienste beziehen, enthalten sein.
Authority Key Identifier	N	1.3.6.1.5.5.7.48.2=http://pki.hessen.de/CA-1-Hessen*NN*.crt Optional können noch Einträge, die sich auf interne Verzeichnisdienste beziehen, enthalten sein. 1.3.6.1.5.5.7.48.1=http://ocsp.hessen.de/ocsp

N: nicht-kritische (non-critical) Erweiterung
J: kritische (critical) Erweiterung