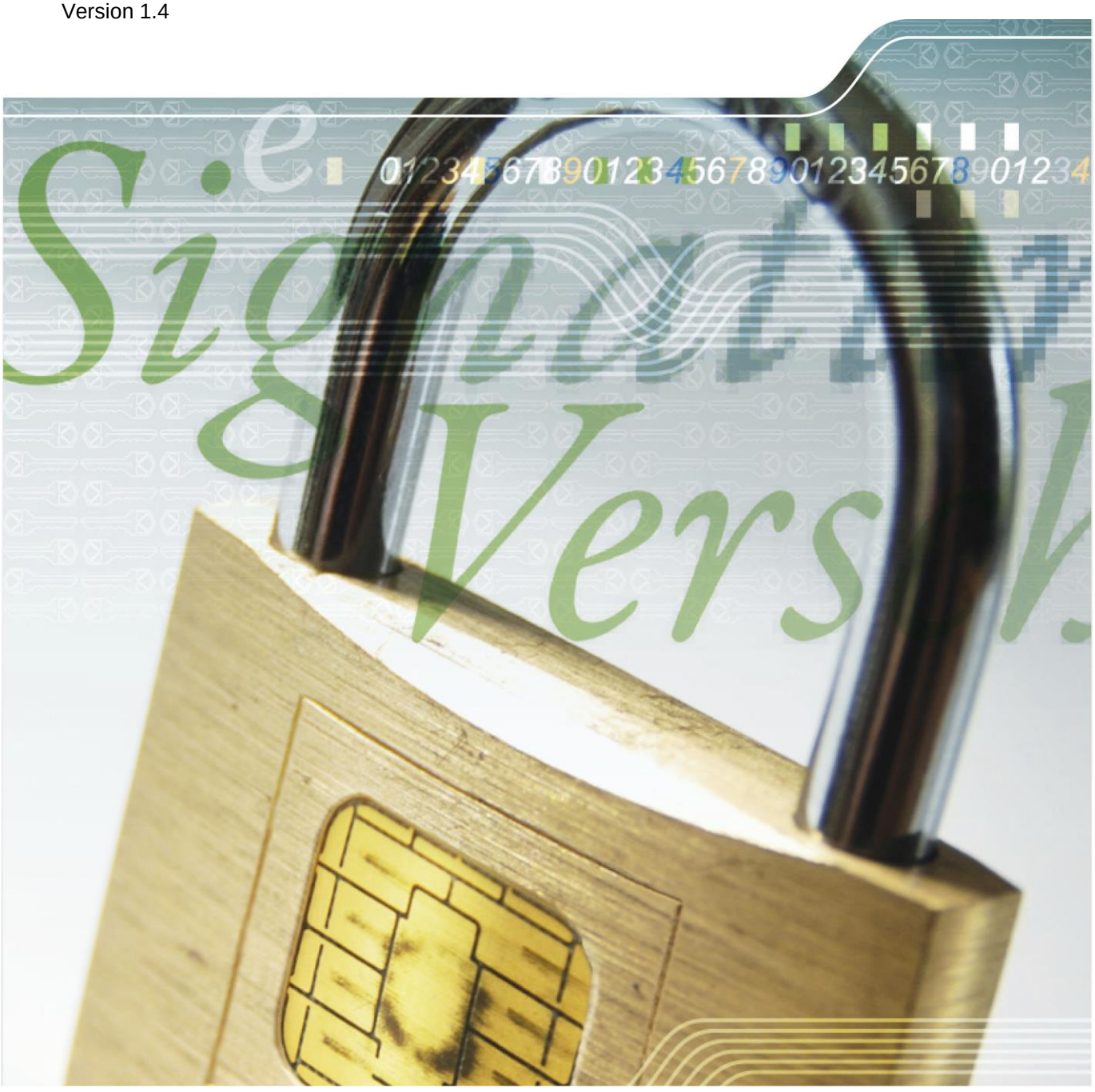
STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

Sachsen PKI
X.509 Public Key Infrastructure der Landesverwaltung Sachsen

Version 1.4



- Sachsen PKI
- X.509 Public Key Infrastructure der Landesverwaltung Sachsen
- Zertifikatsrichtlinie Certificate Policy (CP) & Erklärung zum Zertifizierungsbetrieb Certification Practice Statement (CPS)
- Version 1.4 – final

Dokumentenkontrolle:

Titel:	Sachsen PKI X.509 Public Key Infrastructure der Landesverwaltung Sachsen Zertifikatsrichtlinie / Certificate Policy (CP) & Erklärung zum Zertifizierungsbetrieb / Certification Practice Statement (CPS)
Beschreibung:	Überblick über die Richtlinien, Prozesse und Prozeduren der Sachsen PKI
RFC Schema:	RFC 3647 (Certificate Policy and Certification Practices Framework)

Versionskontrolle:

Version	Datum	Kommentar
1.0 final	23.09.2011	Erstellung Version 1.0 final
1.1 final	01.06.2012	Redaktionelle Änderungen
1.2 final	03.11.2014	Redaktionelle Änderungen Sachsen PKI (2)
1.3 final	19.01.2015	Redaktionelle Änderungen - Kontaktdaten
1.4 final	9.8.2017	Redaktionelle Änderungen

Inhaltsverzeichnis

1. Einleitung 3

1.1. Überblick 4
1.2. Dokumententitel und Identifikation 5
1.3. Teilnehmer und Instanzen 6
1.4. Anwendungsbereich von Zertifikaten 8
1.5. Verwaltung der Richtlinien 8
1.6. Definitionen und Abkürzungen 9

2. Publikationen und Informationsdienste 11

2.1. Verzeichnis- und Informationsdienste 11
2.2. Publikation von Zertifizierungsinformationen 11
2.3. Veröffentlichungsintervall 12
2.4. Zugang zu den Informationsdiensten 12

3. Identifikation und Authentifikation 13

3.1. Namen 13
3.2. Identitätsprüfung bei Neuantrag 16
3.3. Identifikation und Authentisierung bei Zertifikatserneuerung 18
3.4. Identifikation und Authentisierung bei Zertifikatsrückruf 18

4. Betriebliche Anforderungen an den Zertifikatslebenszyklus 19

4.1. Zertifikatsantrag 20
4.2. Prozess für die Antragsbearbeitung 20
4.3. Zertifikatsausgabe 21
4.4. Zertifikatsannahme 21
4.5. Schlüsselpaar- und Zertifikatsverwendung 22
4.6. Zertifikatserneuerung 23
4.7. Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung 25
4.8. Zertifikatssperrung und -suspendierung 25
4.9. Auskunftsdienste für den Zertifikatsstatus 27
4.10. Schlüsselhinterlegung und -wiederherstellung 28

5. Einrichtungen, Sicherheitsmanagement, organisatorische und betriebliche Sicherheitsmaßnahmen 29

5.1. Physikalische- und Umgebungssicherheit 29
5.2. Organisatorische Sicherheitskontrollen 30
5.3. Sicherheitsmaßnahmen für das Personal 31
5.4. Überwachung von sicherheitskritischen Ereignissen 32
5.5. Archivierung von Protokolldaten 34
5.6. Schlüsselwechsel der Zertifizierungsstellen 36
5.7. Kompromittierung und Wiederanlauf nach Katastrophen 36

6. Technische Sicherheitsmaßnahmen 39

6.1. Schlüsselpaarerzeugung und Installation 39
6.2. Schutz des privaten Schlüssels und kryptographische Module 41
6.3. Weitere Aspekte für die Verwaltung von Schlüsselpaaren 43
6.4. Aktivierungsdaten 43

6.5. Sicherheitsmaßnahmen für Computer 43
6.6. Technische Kontrollen für den gesamten Lebenszyklus 44
6.7. Sicherheitsmaßnahmen im Netz 44
6.8. Zeitstempel 45

7. Zertifikats- und CRL Profil 46

7.1. Zertifikatsprofil 46
7.2. CRL Profil 48
7.3. OCSP Profil 49

8. Auditierung und Überprüfung der Konformität 50

8.1. Frequenz und Umstand der Überprüfung 50
8.2. Identität und Qualifikation des Prüfers/Auditors 50
8.3. Verhältnis des Prüfers zur überprüften Entität 50
8.4. Von der Überprüfung abgedeckte Bereiche 50
8.5. Maßnahmen bei Nichterfüllung oder Abweichen von der Konformität 51
8.6. Kommunikation der Prüfergebnisse 51

9. Weitere rechtliche und geschäftliche Regelungen 52

9.1. Gebühren 52
9.2. Finanzielle Verantwortung 52
9.3. Vertraulichkeit von Geschäftsinformationen 53
9.4. Datenschutz (personenbezogen) 53
9.5. Urheberrechte 54
9.6. Verpflichtungen 54
9.7. Gewährleistung 55
9.8. Haftungsbeschränkung 55
9.9. Haftungsfreistellung 55
9.10. Inkrafttreten und Aufhebung 55
9.11. Individuelle Benachrichtigung und Kommunikation mit Teilenehmern 56
9.12. Ergänzungen der Richtlinie 56
9.13. Schiedsverfahren 56
9.14. Gerichtsstand 56
9.15. Konformität zum geltenden Recht 57
9.16. Weitere Regelungen 57
9.17. Andere Regelung 58

1. Einleitung

Das vorliegende Dokument beschreibt die Vertrauenswürdigkeit der über die Sachsen PKI ausgegebenen elektronischen Zertifikate und des in diesem Rahmen durch den Freistaat Sachsen betriebenen Zertifizierungsdienstes. Mit Teilnahme an den Zertifizierungsdiensten der Sachsen PKI akzeptieren die Nutzer die in diesem CP/CPS aufgeführten Bedingungen und Regularien.

Der Begriff „Certificate Policy“ (CP), definiert im X.509 Standard, steht für die Gesamtheit der Regeln und Vorgaben, welche die Vertrauenswürdigkeit und Anwendbarkeit eines Zertifikatstyps festlegen. Die Zielsetzung einer „Certificate Policy“ wird im RFC 3647 („Certificate Policy and Certification Practices Framework“) ausführlich diskutiert. Die CP ist eine Entscheidungshilfe für den Zertifikatsnutzer, ob einem bestimmten Zertifikat bei einer Zertifikats-Anwendung vertraut werden kann.

Insbesondere soll die CP darlegen:

- welche technischen und organisatorischen Anforderungen an die bei der Ausstellung der Zertifikate eingesetzten Systeme und Prozesse gestellt werden,
- welche Vorgaben für die Anwendung der Zertifikate sowie im Umgang mit den zugehörigen Schlüsseln und Signaturerstellungseinheiten (z.B. HSMs bzw. Chipkarten) gelten,
- welche Bedeutung den Zertifikaten und zugehörigen Anwendungen zukommt, d.h. welche Sicherheit, Beweiskraft, oder rechtliche Relevanz die mit ihnen erzeugten Signaturen bzw. verschlüsselten Texte besitzen.

Das Konzept eines „Certification Practice Statement (CPS)” wurde von der American Bar Association (ABA) entwickelt und ist in deren „Digital Signature Guidelines“ (ABA Guidelines) aufgeführt. Das CPS ist eine detaillierte Beschreibung des Zertifizierungsbetriebs der Organisation. Aus diesem Grund stellen Organisationen, die eine oder mehrere Zertifizierungsstellen betreiben, in der Regel auch ein CPS zur Verfügung. Im Rahmen einer unternehmensweiten PKI ist das CPS für Organisationen ein adäquates Mittel um sich selbst zu schützen, sowie Geschäftsvorfälle zwischen Zertifikatsnehmern und vertrauenden Parteien darzustellen.

Die Dokumentenstruktur orientiert sich an die im RFC 3647 angegebenen Empfehlungen. Entsprechend den Vorgaben des RFC 3647 legt CP/CPS der Sachsen PKI die Vorgehensweise dar, die der Zertifizierungsdienst bei der Beantragung, Generierung, Auslieferung, Verwaltung und Sperrung der Zertifikate und im Falle einer möglichen Zertifizierung von untergeordneten Zertifizierungsstellen (SubCAs) anwendet.

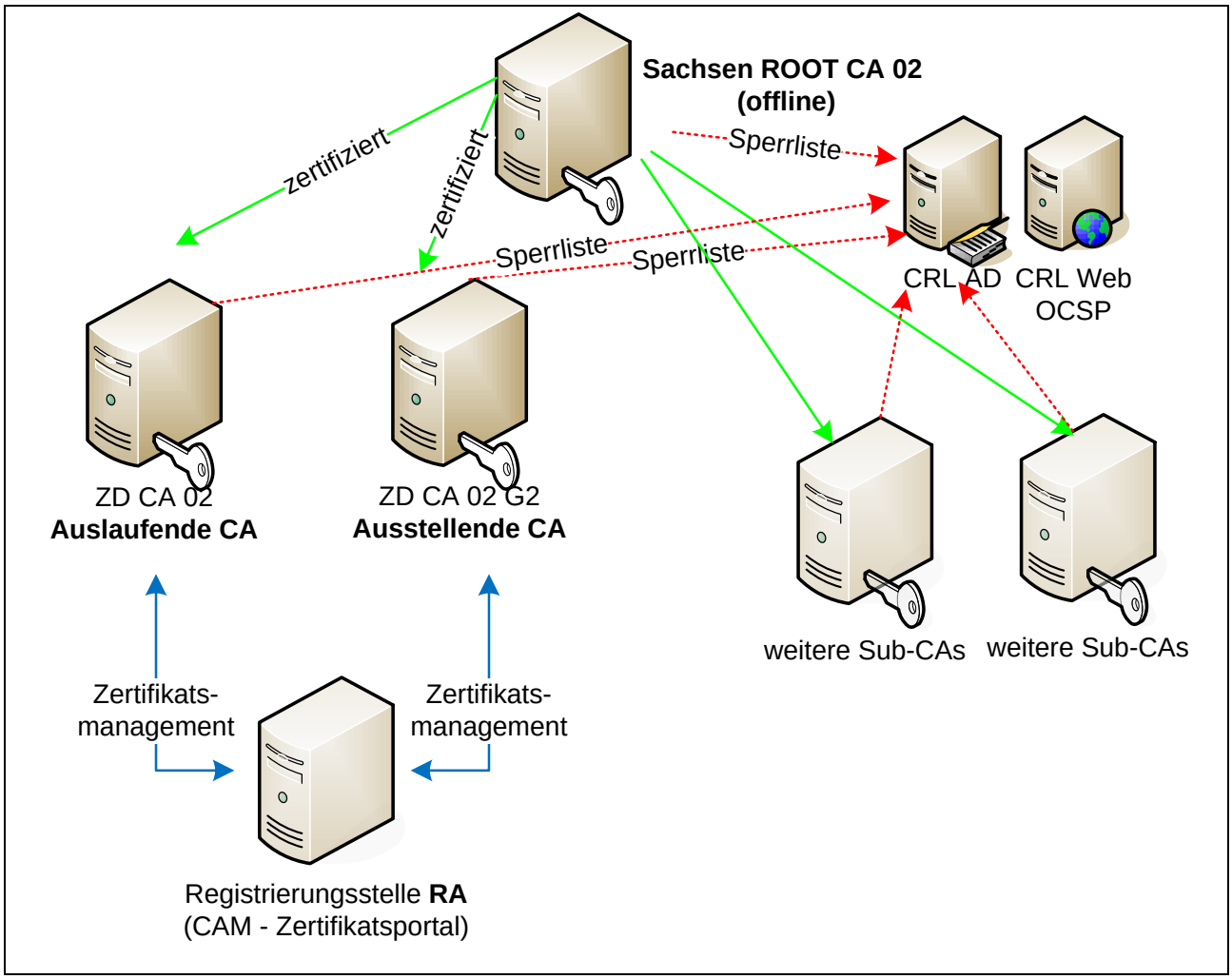
Der Inhalt lehnt sich an die Sicherheitsleitlinie der Wurzelzertifizierungsstelle der Verwaltungs-PKI des Bundes an, unterwirft sich aber nicht den dortigen Vorgaben im Sinne einer untergeordneten CA.

Aufgrund der Anforderung einer vereinfachten Dokumentenverwaltung wurden die CP (Certificate Policies) und CPS (Certification Practice Statement) in einem zentralen Dokument als CP/CPS zusammengefasst. Dieses Dokument beschreibt die Zertifikatsrichtlinie und die Erklärung zum Zertifizierungsbetrieb der Sachsen PKI im Freistaat Sachsen. Das CP/CPS ist kostenfrei und öffentlich im Internet verfügbar.

1.1. Überblick

Die ausstellende Zertifizierungsstelle ZD CA 02 der Sachsen PKI nach CPS Version 1.3 stellt ab Veröffentlichung der Version 1.4 keine Domaincontroller- und Webserverzertifikate aus - der Sperrdienst bleibt bestehen. Mit Ablauf der ausgestellten Zertifikate (max. ein Jahr nach Veröffentlichungsdatum CP/CPS Version 1.4) wird die ausstellende Zertifizierungsstelle ZD CA 02 nach CPS Version 1.3 eingestellt. Die CP/CPS Version 1.3 ist unter folgenden Link weiterhin verfügbar: *http://secure.sachsen.de/pki/cps/SachsenPKI-CP-CPS-V1_3.pdf.* Die Ausgabe von Zertifikate wird nahtlos von der ZD-CA-02-G2 übernommen.

Die Zertifizierungsinfrastruktur der Sachsen PKI ist hierarchisch aufgebaut und basiert auf der Sachsen Root CA 02. Diese Wurzelzertifizierungsstelle bildet die oberste Instanz der PKI (Root CA) und stellt die Zertifikate für untergeordnete CAs aus.



Die von der Wurzelzertifizierungsstelle zertifizierten CA‘s (Certification Authority) bilden die zweite Stufe der PKI-Hierarchie. Sie werden den Organisationen innerhalb der Landesverwaltung zugeordnet, die in eigener Zuständigkeit und Verantwortung eine Windows-Sub-Domäne unter dem Dach des ADS-Verbunds der Landesverwaltung betreiben.

Zertifikate für Systeme im Sächsischen Verwaltungsnetz (SVN) werden zentral von der CA der Domäne zd.sachsen.de („ZD CA“) ausgestellt. Weitere CAs sind für spezielle Anforderungen vorgesehen, aber derzeit nicht in Betrieb. Der ZD-CA ist eine Registrierungsstelle (CAM Zertifikatsportal) vorgeschaltet.

Der Freistaat Sachsen betreibt die Zertifizierungsdienste der Sachsen PKI komplett in eigener Hoheit. Der mit dem Betrieb des SVN2 beauftragte Dienstleistungspartner des Freistaats Sachsen stellt die notwendige Infrastruktur (z.B. Rechenzentrum, Zugangskontrolle und Notstromversorgung) bereit.

Zwei netzwerkbasierte „Hardware-Sicherheitsmodule“ (Hardware Security Module), kurz HSM, übernehmen die Schlüsselgenerierung und -verwaltung für die Sachsen PKI Zertifizierungsstellen.

Weitergehende Informationen zur PKI-Architektur können auf Wunsch angefordert werden. Die Kontaktinformationen der zuständigen Ansprechpartner sind dem Abschnitt 1.5.2 Kontaktpersonen zu entnehmen.

1.2. Dokumententitel und Identifikation

Es handelt sich hierbei um die Zertifikatsrichtlinie und die Erklärung zum Zertifizierungsbetrieb der Sachsen PKI im Freistaat Sachsen. Ein eindeutiger ASN.1 Object Identifier (OID) ist diesem Dokument zugewiesen.

Die OID im Nummernkreis der „Private Enterprise Number“ (PEN) des Freistaats Sachsen ist bei der IANA.ORG registriert, siehe auch: *http://www.iana.org/assignments/enterprise-numbers*

- **Sachsen Private Enterprise OID:** 1.3.6.1.4.1.7848
  OID Beschreibung: Sächsische Staatskanzlei Private Enterprise Number
- **Sachsen PKI OID:** 1.3.6.1.4.1.7848.1
  OID Beschreibung: Namensraum der X.509 PKI Dienste der Sachsen PKI im Freistaat Sachsen
- **Sachsen PKI CP/CPS OID:** 1.3.6.1.4.1.7848.1.10.1
  OID Beschreibung: Ausstellererklärung der Sachsen PKI

Der CP/CPS Titel lautet:

- Sachsen PKI
- X.509 Public Key Infrastructure des Freistaats Sachsen
- Zertifikatsrichtlinie / Certificate Policy (CP) & Erklärung zum Zertifizierungsbetrieb / Certification Practice Statement (CPS)

Die Veröffentlichung der CP/CPS Dokumentation der Sachsen PKI für Zertifikatsnehmer und vertrauende Parteien erfolgt unter: *http://secure.sachsen.de/pki/cps*

1.3. Teilnehmer und Instanzen

Die Teilnehmer der Sachsen PKI sind grundsätzlich in 4 Teilnehmergruppen klassifiziert. Jeder dieser teilnehmenden Gruppen bietet PKI Dienste und Ressourcen an oder nutzt PKI Dienste und Ressourcen.

Zertfizierungsstelle oder Certificate Authority (CA):

- Ausstellen von Zertifikaten,
- Sperren von Zertifikaten.

Registrierungsstelle oder Registration Authority (RA):

- Identifizierung von Benutzern oder Maschinen,
- Registrierung von Benutzern oder Maschinen,
- Beantragung einer Zertifikatsanforderung für andere Benutzer,
- Beantragung einer Sperranforderung von Zertifikaten.

Zertifikatsnehmer:

- Nutzt Zertifikate und PKI Dienstleistungen.

Vertrauende Parteien:

- Nutzt PKI Dienstleistungen.

1.3.1. Zertifizierungsstellen

Das zweistufige CA Hierarchie-Modell basiert auf:

- Wurzelinstanz (***Root CA***, „Sachsen Root CA 02“) mit einem selbst-signierten CA Zertifikat. Die Sachsen Root CA 02 ist im Regelbetrieb vom Produktionsnetz entkoppelt und unterhält lediglich eine dedizierte Verbindung zu den Hardware Security Modules (HSMs). Alle kryptographischen Operationen der Sachsen Root CA 02 werden durch das HSM ausgeführt bzw. abgesichert. Die Sachsen Root CA 02 stellt CA Zertifikate und Sperrlisten für untergeordnete Zertifizierungsstellen (Issuing bzw. Sub CAs), wie auch für sich selbst aus.
- Ausgebende Zertifizierungsstellen *(**Issuing CAs**, „ZD CA 02“ und „ZD CA 02 G2“)* mit einem von der Sachsen Root CA 02 ausgestellten Zertifikat. Die Issuing CAs sind mit dem Produktionsnetz verbunden und unterhalten ebenso, wie die Sachsen Root CA 02, eine dedizierte Verbindung zu den HSMs. Alle kryptographischen Operationen der Issuing CAs werden durch die HSMs ausgeführt bzw. abgesichert. Die Issuing CAs stellen End-Entitäten Zertifikate und Sperrlisten für die Zertifikatsnehmer aus.

Für die Zertifizierungsstellen sind folgende Lebensdauern von Zertifikaten und Sperrlisten festgelegt:

Sachsen Root CA 02

- Root CA 02 Zertifikat: 21 Jahre
- Root CA 02 CRLs: 27 Wochen (26 Wochen Publikationsintervall und 1 Woche Überlappungszeitraum)

ZD CA 02

- ZD CA 02 Zertifikat: 5 Jahre
- ZD CA 02 CRLs: 10 Tage (7 Tage Publikationsintervall und 3 Tage Überlappungszeitraum)
- ZD CA 02 Delta-CRLs: 4 Stunden

ZD CA 02 G2

- ZD CA 02 G2 Zertifikat: 10 Jahre
- ZD CA 02 G2 CRLs: 10 Tage (7 Tage Publikationsintervall und 3 Tage Überlappungszeitraum)
- ZD CA 02 G2 Delta-CRLs: 4 Stunden

1.3.2. Registrierungsstellen

Die Registrierungsstellen im Sinne dieses CP/CPS sind Instanzen, welche die Zertifikatsnehmer und Antragssteller erfassen, zweifelsfrei eindeutig identifizieren und auch für Zertifikatsnehmer Zertifikate beantragen. Die Registrierung der Zertifikate geschieht in lokalen Registrierungsstellen (LRA). Als Registrierungsstellen der Sub-CAs agieren die bestehenden Organisationen, die auch die normale Nutzerverwaltung der Windows-Domänen und damit die Identifizierung von Zertifikatsinhabern (Server, Clientrechner und Personen) verantwortlich durchführen.

Die Zertifikatsbeantragung für maschinenbezogene Zertifikatstypen erfolgt teilautomatisiert bzw. manuell durch den jeweils zuständigen und Service - verantwortlichen Ansprechpartner des Dienstes bzw. der Maschine.

1.3.3. Zertifikatsnehmer

Zertifikatsnehmer sind End-Entitäten, denen ein Zertifikat durch die Issuing CAs zugewiesen wird. Die Umstände und Rahmenbedingungen der Schlüsselgenerierung als auch die Zertifikatsausgabe unterstehen nicht der Kontrolle des Zertifikatsnehmers, sondern obliegen der Sachsen PKI.

Zertifikatsnehmer im Rahmen dieser PKI können technische Systeme (wie z. B. in Domänen integrierte Maschinen als auch einzelne Maschinen) und Personen sein, denen in der PKI Struktur bestimmte Rollen zugewiesen wurden.

1.3.4. Vertrauende Parteien

Vertrauende Parteien im Sinne des vorliegenden CP/CPS sind alle Personen und Systeme, die mit Hilfe eines Zertifikates mit dessen Inhaber sicher kommunizieren wollen.

1.3.5. Weitere Teilnehmer

Nicht zutreffend.

1.4. Anwendungsbereich von Zertifikaten

Die ordnungsgemäße Verwendung von Schlüsseln und Zertifikaten obliegt der Verantwortung des Zertifikatsnehmers und der vertrauenden Partei.

1.4.1. Zulässige Anwendung von Zertifikaten

Die im Rahmen dieser CP/CPS ausgestellten Zertifikate sind ausschließlich für den dienstlichen Gebrauch bestimmt.

Die zulässige Anwendung wird für jedes Zertifikatsprofil in den Feldern Schlüsselverwendung und erweiterte Schlüsselverwendung definiert.

1.4.2. Unzulässige Anwendung von Zertifikaten

Die Zertifikatsnutzung innerhalb der Sachsen PKI ist beschränkt und nur für den Einsatz der vorgegebenen Anwendungsbereiche zulässig. Root-CA Zertifikate dürfen nur für die Signierung von CA Schlüsseln und Sperrlisten herangezogen werden.

Eine Anwendung der Zertifikate für den privaten bzw. anderweitigen nicht dienstlichen Gebrauch ist ebenso untersagt, wie auch die Nutzung dieser Zertifikate für andere Anwendungszwecke abweichend von 1.4.1 Zulässige Anwendungen von Zertifikaten.

Jegliche weitere Zertifikatsnutzung ist untersagt, insbesondere die Zertifizierung weiterer, untergeordneter Zertifizierungsstellen ist ausschließlich der Sachsen Root CA 02 vorbehalten und nur mit Zustimmung der für die Sachsen Root CA 02 verantwortlichen PKI-Aufsicht / Projektleitung Sachsen PKI möglich.

1.5. Verwaltung der Richtlinien

1.5.1. Organisation

Der Freistaat Sachsen, vertreten durch das Sächsische Staatsministerium des Innern (SMI) ist die verantwortliche Organisation für die Herausgabe des CP/CPS.

> Sächsisches Staatsministerium des Innern
> Wilhelm-Buck-Straße 4
> 01097 Dresden

1.5.2. Kontaktpersonen

Folgende Personen sind Ansprechpartner für die Verwaltung des CP/CPS der Sachsen PKI:

- **PKI-Aufsicht / Projektleitung Sachsen PKI**
  Sächsisches Staatsministerium des Innern
  Referat 61 – Grundsatz- und Rechtsangelegenheiten IT und E-Government,
  Finanzen, Gremienbetreuung
  E-Mail: pki@sachsen.de

1.5.3. Verantwortliche Personen für das CP/CPS

Die die PKI-Aufsicht / Projektleitung Sachsen PKI ist verantwortlich für das CP/CPS und die begleitende Dokumentation. Die Kontaktdaten sind im Abschnitt 1.5.2 Kontaktpersonen aufgeführt.

1.5.4. CPS Genehmigungsverfahren

Die PKI-Aufsicht / Projektleitung Sachsen PKI ist verantwortlich für die Freigabe dieser CP/CPS. Die CP/CPS Dokumentation wird fortwährend, mindestens jedoch einmal innerhalb eines Kalenderjahres bzw. sofort bei möglichen weiteren Implementierungen oder technischen Änderungen, auf Konformität und Aktualität hin untersucht und ggf. angepasst.

Wenn durch spezielle unabweisbare Anforderungen einzelner SubCAs umfangreiche Änderungen der CP/CPS notwendig werden, entscheidet die PKI-Aufsicht / Projektleitung Sachsen PKI, ob das zentrale CP/CPS bei gleichbleibender OID angepasst wird oder mit neuer OID eine eigene CP/CPS-Version der SubCA zu erstellen ist. In einem solchen Ausnahmefall sind die Abweichungen von der zentralen Fassung zu kennzeichnen und die Veröffentlichung an den Verteilpunkten parallel zur zentralen Fassung sicherzustellen.

1.6. Definitionen und Abkürzungen

- **ABA (American Bar Association)** – Verband der amerikanischen Rechtsanwälte, Richter
- **ASN.1 (Abstract Syntax Notation)** – Abstrakte Syntaxnotation Nummer 1, Datenbeschreibungssprache
- **C (Country)** – Landesobjekt (Teil des X.500 Distinguished Name), für Deutschland C=DE
- **CA (Certification Authority)** – Zertifizierungsstelle
- **CN (Common Name)** – Namensobjekt (Teil des X.500 Distinguished Name)
- **CP (Certificate Policy)** – Zertifikatsrichtlinie
- **CPS (Certification Practice Statement)** – Zertifizierungsbetrieb
- **CRL (Certificate Revocation List)** – Liste, in der eine Zertifizierungsstelle die von ihr ausgestellten Zertifikate, die gesperrt aber noch nicht abgelaufenen sind, veröffentlicht
- **CSR (Certificate Signing Request)** – Signierte Zertifikatsanforderung
- **DN (Distinguished Name)** – Eindeutiger Name basiert auf der X.500 Namensbildung
- **DNS (Domain Name System)** – Standard für Internet Namen
- **FIPS (Federal Information Processing Standard)** – Kryptographiestandard der US Behörden (FIPS 140-2 Sicherheitsanforderungen für Kryptographische Module)

- **HSM (Hardware Security Module)** – Hardwarekomponente, die sicherheitsrelevante Informationen wie Daten und kryptographische Schlüssel sicher speichert und verarbeitet
- **IETF (Internet Engineering Task Force)** – Projektgruppe für die technische Weiterentwicklung des Internets. Spezifiziert Standards in Form von RFCs**.**
- **IP (Internet Protocol)** – Internetprotokoll
- **ISO (International Organization for Standardization)** – Internationale Normungsstelle
- **ITU (International Telecommunications Union)** – Standardisierungsgremium, hat auch X.509 spezifiziert
- **LDAP (Lightweight Directory Access Protocol)** – Zugriffsprotokoll für Verzeichnisdienste
- **NIST (National Institute of Standards and Technology)** – Normungsstelle der Vereinigten Staaten
- **O (Organization)** – Objekt für die Organisation (Teil des X.500 Distinguished Name)
- **OID (Object Identifier)** – Object Identifikator, eindeutige Referenz zu Objekten im OID Namensraum
- **OU (Organizational Unit)** – Objekt für die Organisationseinheit (Teil des X.500 Distinguished Name)
- **PIN (Personal Identification Number)** – Geheimzahl zur Authentisierung eines Individuums z.B. gegenüber einer Chipkarte
- **PKCS (Public Key Cryptographic Standard)** – Serie von Quasi-Standards für kryptographische Operationen spezifiziert durch RSA
- **PKI (Public Key Infrastructure)** – System zur Ausstellung, Verteilung und Prüfung von elektronischen Identitätsnachweisen (Zertifikaten)
- **PKIX (Public Key Infrastructure eXchange)** – eine Serie von Spezifikationen der IETF im Umfeld von digitalen Zertifikaten nach X.509 Spezifikation
- **RA (Registration Authority)** – Registrierungsstelle
- **RFC (Request for Comment)** – Quasi Internet-Standard ausgegeben durch die IETF
- **URL (Uniform Resource Locator)** – Ressourcen Lokation im Internet
- **X.500** – Protokolle und Dienste für ISO konforme Verzeichnisse
- **X.509** – Authentifikationsmethode für X.500 Verzeichnisse
- **X.509v3** – Aktuell gültiger PKI Zertifikatsstandard

2. Publikationen und Informationsdienste

2.1. Verzeichnis- und Informationsdienste

Für öffentliche Informationen wie Sachsen PKI CA Zertifikate, CRLs und CP/CPS Dokumentation wird die Webseite *http://secure.sachsen.de/pki* als Informationsdienst genutzt. Ebenso werden diese Informationen mit Ausnahme der CP/CPS Dokumentation durch das Active Directory des SVN als Verzeichnisdienst veröffentlicht.

2.2. Publikation von Zertifizierungsinformationen

Die fortlaufende Publikation der CA Sperrlisten auf den Sachsen PKI Web Servern und in das Active Directory des SVN wird durch die Issuing CAs automatisiert durchgeführt; die Publikation der Sachsen Root CA 02 CRLs wird im Gegensatz dazu manuell durch die für die Sachsen PKI zuständigen Mitarbeiter auf den Web Servern und im Active Directory ausgeführt, da eine netztechnische Trennung bzw. ein offline Betrieb der Root CA gegeben ist. CA Zertifikate und die CP/CPS Dokumentation werden durch die PKI-Aufsicht / Projektleitung Sachsen PKI freigegeben und auf den entsprechenden Webseiten eingestellt.

Folgende Veröffentlichungsorte werden verwendet:

- Sachsen PKI CP/CPS:
  - *http://secure.sachsen.de/pki/cps/*
- Sachsen Root-CA-02 Sperrlisten:
  - *ldap:///CN=Sachsen%20Root%20CA%2002,CN=ROOT-CA-02,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=sachsen,DC=de?certificateRevocationList?base?objectClass=cRLDistributionPoint*
  - *http://secure.sachsen.de/pki/crl/Sachsen%20Root%20CA%2002.crl*
- ZD-CA-02 Sperrlisten:
  - *ldap:///CN=ZD%20CA%2002,CN=ZD-CA-02,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=sachsen,DC=de?certificateRevocationList?base?objectClass=cRLDistributionPoint*
  - *http://secure.sachsen.de/pki/crl/ZD%20CA%2002.crl*
- ZD-CA-02-G2 Sperrlisten:
  - *ldap:///CN=ZD%20CA%2002%20G2,CN=ZD-CA-02-G2,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=sachsen,DC=de?certificateRevocationList?base?objectClass=cRLDistributionPoint*
  - *http://secure.sachsen.de/pki/crl/ZD%20CA%2002%20G2.crl*
- Sachsen Root-CA-02 Zertifikat:

- *ldap:///CN=Sachsen%20Root%20CA%2002,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=sachsen,DC=de?cACertificate?base?objectClass=certificationAuthority*
- *http://secure.sachsen.de/pki/aia/Sachsen%20Root%20CA%2002.crt*

- ZD-CA-02 CA Zertifikat:
  - *ldap:///CN=ZD%20CA%2002,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=sachsen,DC=de?cACertificate?base?objectClass=certificationAuthority*
  - *http://secure.sachsen.de/pki/aia/ZD%20CA%2002.crt*
- ZD-CA-02-G2 CA Zertifikat:
  - *ldap:///CN=ZD%20CA%2002,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=sachsen,DC=de?cACertificate?base?objectClass=certificationAuthority*
  - http://secure.sachsen.de/pki/aia/ZD%20CA%2002%20G2.crt

- Sachsen PKI OCSP:
  - *http://secure.sachsen.de/ocsp*

2.3. Veröffentlichungsintervall

Die Veröffentlichung der Zertifikatsrichtlinie und der Erklärung zum Zertifizierungsbetrieb der Sachsen PKI erfolgt jeweils nach ihrer Erstellung bzw. einer Aktualisierung. Eine Benachrichtigung der bis zu diesem Zeitpunkt bereits vertrauenden Parteien / Zertifikatsteilnehmer über eine mögliche Aktualisierung findet nicht statt.

Die Veröffentlichung der Sachsen PKI CA Zertifikate erfolgt einmalig nach der Installation der Sachsen PKI Zertifizierungsstellen. Eine erneute Publikation erfolgt nur bei Ablauf bzw. Erneuerung der CA Zertifikate. Eine Benachrichtigung der bis zu diesem Zeitpunkt bereits vertrauenden Parteien / Zertifikatsteilnehmer über eine mögliche Aktualisierung findet nicht statt.

CRL oder Sperrlisten werden nach vorgeschriebenem Publikationsintervall erzeugt und anschließend mit technisch bedingten kurzen Latenzzeiten auf den PKI Web Diensten und in das Active Directory publiziert.

- CRLs durch die Root CA ausgestellt:
  - Root CA jeweils alle 26 Wochen mit einer Überlappung von max. 1 Woche
- CRLs durch die Issuing CAs ausgestellt:
  - ZD-CA-02 und ZD-CA-02-G2 jeweils alle 7 Tage mit einer Überlappung von max. 3 Tagen
  - alternativ Deltasperrlisten (ZD-CA-02 und ZD-CA-02-G2 4 Stunden)

2.4. Zugang zu den Informationsdiensten

Der Zugriff auf die CA Zertifikate, Sperrlisten und die CP/CPS Dokumentation ist nicht eingeschränkt und daher öffentlich (siehe auch die Definition der Veröffentlichungsorte in Abschnitt 2.2. Publikation von Zertifizierungsinformationen).

3. Identifikation und Authentifikation

3.1. Namen

3.1.1. Namensform

Das X.509 Zertifikatssubject in den CA-Zertifikaten für Sachsen PKI Zertifikatsnehmer ist wie in den folgenden Tabellen dargestellt spezifiziert. Der Einsatz von Zertifikatssubjects für die Benennung im Subject Name Field erlaubt die Eindeutigkeit der Namensvergabe von Zertifizierungsstellen innerhalb des Active Directory des SVN im Rahmen der Sachsen PKI.

Das Schema für die Namensform ist bei allen ausgestellten Zertifikaten der Sachsen PKI identisch und folgt untenstehendem Regelwerk:

- CN = [Common Name],
- OU = [Organizational Unit],
- OU = [Organizational Unit],
- OU = [Organizational Unit],
- O = [Organization],
- C = [Country],
- DC = [Domain Component],
- E-Mail = [RFC822 Naming Context].

In der Zertifizierungspraxis werden nur die (Namens-) Attribute festgelegt, die zur Eindeutigkeit der Namen im Bereich der Zertifizierungsstellen notwendig sind. Der Freistaat Sachsen betreibt die Zertifizierungsstellen in einer zweistufigen (2-tier) Architektur.

Das Zertifikatssubject der selbst-signierten Sachsen Root CA 02 lautet:

Attribut	Wert
Common Name (CN)	Sachsen Root CA 02
Organization (O)	Landesverwaltung Sachsen
Country (C)	DE

Die Subjects in den durch die Sachsen Root CA 02 ausgestellten Zertifikaten der ausgebenden CAs der Sachsen PKI lauten:

Attribut	Wert
Common Name (CN)	ZD CA 02
Organizational Unit (OU)	Zentrale Dienste
Organization (O)	Landesverwaltung Sachsen
Country (C)	DE

Attribut	Wert
Common Name (CN)	ZD CA 02 G2
Organizational Unit (OU)	Zentrale Dienste
Organization (O)	Landesverwaltung Sachsen
Country (C)	DE

Weitere als die hier genannte ausgebenden CAs werden derzeit nicht betrieben.

3.1.2. Anforderung an die Bedeutung von Namen

Der Distinguished Name muss den Zertifikatnehmer eindeutig identifizieren. Ist der DN nicht ausreichend, kann zur Einhaltung der Eindeutigkeit eines Namens auch der Subject Alternative Name herangezogen werden. Bei der Namensvergabe sind folgenden Regelungen wirksam:

- Zertifikate dürfen nur auf einen zulässigen Namen des Zertifikatnehmers ausgestellt werden.
  - Bei den Authentifikationszertifikaten für Benutzer ist es der Nachname und Vorname im Common Name und der UPN (User Principle Name) im Subject Alternative Name Feld des Zertifikatsnehmers.
  - Bei den Verschlüsselungs- und Signaturzertifikaten für Benutzer ist es der Nachname und Vorname im Common Name und die E-Mail-Adresse im Subject Feld (E=) des Zertifikatsnehmers.

- Bei den Authentifikationszertifikaten für Computer bzw. Web Server ist es der Computer DNS Name oder die Web Server URL im Common Name im DN sowie der Computer DNS Name oder die Web Server URL im Subject Alternative Name Feld des Zertifikatsnehmers.

- Der CN für Benutzerzertifikate ist grundsätzlich nach der Systematik „Nachname, Vorname“ aufzubauen, der UPN soll grundsätzlich der E-Mail-Adresse des Benutzers entsprechen. Näheres ist dem Namenskonzept des Active Directory im SVN zu entnehmen.
- Der DN der Sachsen PKI Zertifizierungsstellen wird durch die Namensobjekte Common Name, Organizational Unit gebildet. Eine Eindeutigkeit des DNs ist mit diesen zur Verfügung stehenden Namensobjekten im Active Directory zu gewährleisten.
- Der DN der Authentifikationszertifikate wird durch die Namensobjekte Common Name, Organizational Unit, Domain Component gebildet. Eine Eindeutigkeit des DNs ist mit diesen zur Verfügung stehenden Namensobjekten im Active Directory zu gewährleisten.
- Der DN der Verschlüsselungs- und Signaturzertifikate wird durch die Namensobjekte Common Name, Organizational Unit, Domain Component gebildet. Eine Eindeutigkeit des DNs ist mit diesen zur Verfügung stehenden Namensobjekten im Active Directory zu gewährleisten.
- Der alternative Name in den Verschlüsselungs- und Signaturzertifikaten enthält die E-Mail Adresse des Inhabers in der Form, wie sie vom E-Mail-System vorgegeben wird z.B.
  <Vorname>.<Nachname>@<Ressort- oder Dienststellenkürzel>.sachsen.de.
- Der alternative Name in den Authentifikationszertifikaten enthält den User Principle Name des Inhabers in der Form
  <Anmeldename>@<Active Directory DNS / Kerberos Domain>.
- Der alternative Name in den Authentifikationszertifikaten für Machinen enthält den DNS Namen der Maschine bzw. die Web Server URL in der Form
  <Maschinenname>.<Active Directory DNS Domain>.
- Jedem Zertifikat wird eine eindeutige Seriennummer zugeordnet, welche eine eindeutige und unveränderliche Zuordnung zum Zertifikatnehmer ermöglicht.
- Subject Alternative Names sind zulässig. Der Einsatz von Wildcards (*) ist verboten.

3.1.3. Anonymität und Pseudonymität von Zertifikatsnehmern

Abgesehen von notwendigen technischen Konten oder auch in Ausnahmefällen Gruppenzertifikaten sind Zertifikatsnehmer (Personen und / oder Maschinen) nicht anonym, noch werden zur Kennung von Zertifikatsnehmern Pseudonyme verwendet. Jedem Zertifikatsnehmer (Personen und / oder Maschinen) können daher die Zertifikate eindeutig zugeordnet werden.

3.1.4. Regeln zur Interpretation verschiedener Namensformen

Die ausgewiesenen Zertifikatsubjects im Zertifikatsprofil folgen dem X.509 Standard. Die verwendeten E-Mail Adressen und UPN Einträge im Zertifikatsprofil folgen dem RFC 822 Regelwerk. UPN Namensinformationen müssen UTF-8 encodiert vorliegen.

3.1.5. Eindeutigkeit von Namen

Das komplette Subject in den von der Sachsen PKI ausgestellten Zertifikaten erlaubt die Eindeutigkeit von Namen sowohl der Sachen PKI Zertifizierungsstellen als auch der Namen für die Zertifikatsnehmer.

Eine zusätzliche Kennung im alternativen Namensfeld, nämlich die eindeutige E-Mail Adresse, UPN Namen und Maschinen DNS Namen, sowie eine eindeutige Seriennummer in den Zertifikaten, berücksichtigt diesen Aspekt.

Es wird von den zuständigen Instanzen der Sachsen PKI keine gesonderte explizite Prüfung auf Eindeutigkeit der im Rahmen des Beantragungsprozesses übermittelten Namen durchgeführt bzw. zugesagt, sondern eine vorherige Prüfung durch vorgelagerte technische Systeme bzw. organisatorische Regelungen außerhalb der Zuständigkeit und Verantwortung der Sachsen PKI angenommen. Gleichwohl wird im Rahmen der Genehmigung von Zertifikatsanforderungen versucht, eine Eindeutigkeit der verwendeten Namen nach bestem Wissen und Gewissen zu gewährleisten – was jedoch in keiner Art und Weise als Eigenschaft des Zertifizierungsstellendienstes zugesagt wird.

3.1.6. Erkennung, Authentifikation und Rolle von Warenzeichen

In der Regel beschränkt sich das Zertifikatssubject auf natürliche Personen und Maschinen und hat somit keine Relevanz in der Anerkennung von Warenzeichen. Grundsätzlich sind der Zertifikatsnehmer und auch der Zertifizierungsstellenbetreiber verpflichtet, aufgrund der teilautomatisierten Ausstellung von End-Entitäten Zertifikaten sicherzustellen, dass der Schutz von Warenzeichen gewährleistet wird.

3.2. Identitätsprüfung bei Neuantrag

3.2.1. Verfahren zur Überprüfung des Besitzes von privaten Schlüsseln

Schlüsselpaare können durch die Zertifikatnehmer der Sachsen PKI lokal (ausschließlich für Maschinenzertifikate) oder wie Nutzerzertifikate generiert werden. Für Nutzerzertifikate sind sichere Schlüsselerstellungseinheiten (Smartcard, Hardware Sicherheitsmodule über CA Portal) zu nutzen. Der Besitznachweis für die privaten Schlüssel erfolgt durch die Signierung (mit dem privaten Schlüssel) des PKCS#10-Zertifikatsrequests. Der Certificate Signing Request (CSR) ist die Basis der Überprüfung von privaten Schlüsseln.

Die Schlüsselpaare der Sachsen PKI Zertifizierungsstellen werden ausschließlich durch Hardware Sicherheitsmodule generiert und über eine starke Authentifizierung im Rahmen eines Vier- bzw. Mehr-Augen Prinzips gesichert. Der Besitznachweis für die privaten Schlüssel zu den CA Zertifikaten erfolgt durch die Signierung (mit dem privaten Schlüssel) des PKCS#10-Zertifikatsrequests. Der Certificate Signing Request oder CSR ist die Basis der Überprüfung von privaten Schlüsseln.

3.2.2. Authentifikation der Organisation

Eine Prüfung der Organisationszugehörigkeit, die über die Prüfung der Zugehörigkeit des Antragstellers zum AD-Verbund der Landesverwaltung herausgeht, findet nicht statt.

3.2.3. Authentifikation von Zertifikatsnehmern

Für die Erstausstattung von Zertifikaten für Benutzer findet eine Identitätsprüfung durch die Registrierungsstelle statt. Hierbei werden die notwendigen Maßnahmen ergriffen um die Identität eines Antragsstellers eindeutig festzustellen.

Für teilnehmende Maschinen wird im Falle einer teilautomatisierten Ausgabe von Zertifikaten die Authentifizierung durch ein valides Maschinen - Kerberoskonto in der der Sachsen PKI angeschlossenen Active Directory Domäne durchgeführt.

Für teilnehmende Maschinen wird im Falle einer manuellen Ausgabe von Zertifikaten die Authentifizierung durch die Prüfung des AD-Benutzer Konto des Antragstellers (Service – verantwortliche Stelle) durchgeführt. Hierbei beantragt ein Domänen-oder Organisationseinheiten- Administrator das Zertifikat für die Maschine aus seinem Zuständigkeitsbereich. Eine Beantragung von diesen Zertifikaten kann nur nach erfolgreicher Benutzerauthentifizierung des Administrators bzw. direkter persönlicher Authentifizierung des Administrators gegenüber der für den Betrieb zuständigen Organisationseinheit erfolgen.

3.2.4. Nicht überprüfte Zertifikatsnehmer Information

Es werden nur die Informationen des Zertifikatsnehmers überprüft, welche im Rahmen der Authentifizierung und Identifikation des Zertifikatsnehmers bzw. Antragsteller notwendig sind. Andere Informationen des Zertifikatsnehmers werden nicht berücksichtigt.

3.2.5. Prüfung der Berechtigung zur Antragstellung

Für die Ausgabe von Benutzerzertifikaten findet eine Überprüfung der Berechtigung zur Antragsstellung in Form eines bestehenden und gültigen Benutzerkontos in Verbindung mit einer Mitgliedschaft in einer autorisierenden Gruppe statt.

Für teilautomatisiert erstellte Maschinenzertifikate findet eine Überprüfung der Berechtigung zu Antragstellung in Form eines bestehenden und gültigen Maschinenkontos in Verbindung mit der Mitgliedschaft in einer den Zugriff autorisierenden Gruppe statt.

Es ist somit die Zugehörigkeit in der zulässigen Domäne in Verbindung mit der Gruppenmitgliedschaft ausschlaggebend.

3.2.6. Kriterien für Cross-Zertifizierung und Interoperation

Nicht zutreffend. Zurzeit ist keine Cross-Zertifizierung mit anderen Organisationen geplant.

3.3. Identifikation und Authentisierung bei Zertifikatserneuerung

Die Identifizierung und Authentisierung bei einer routinemäßigen Zertifikatserneuerung mit Schlüsselwechsel (d.h. bei der Ausstellung eines neuen Zertifikates zu einem neuen Schlüsselpaar kurz vor dem regulären Ablauf des alten Zertifikates) entspricht der Identifizierung und Authentifizierung bei der Erst-Registrierung.

3.3.1. Identifikation und Authentisierung bei routinemäßiger Zertifikatserneuerung

Für teilnehmende Maschinen wird im Falle einer teilautomatisierten Erneuerung von Zertifikaten die Authentifizierung durch ein valides und aktives Maschinenkonto in der angeschlossenen Active Directory Domäne durchgeführt.

Für teilnehmende Maschinen wird im Falle einer manuellen Ausgabe von Zertifikaten die Authentifizierung durch die Prüfung des AD-Benutzer Konto des Antragstellers (Service – verantwortliche Stelle) durchgeführt. Hierbei beantragt ein Domänen-oder Organisationseinheiten- Administrator das Zertifikat für die Maschine aus seinem Zuständigkeitsbereich. Eine Beantragung von diesen Zertifikaten kann nur nach erfolgreicher Benutzerauthentifizierung des Administrators bzw. direkter persönlicher Authentifizierung des Administrators gegenüber der für den Betrieb zuständigen Organisationseinheit erfolgen.

3.3.2. Identifikation und Authentisierung bei Zertifikatserneuerung nach erfolgtem Zertifikatsrückruf

Die Identifizierung und Authentifizierung bei einer Zertifikatserneuerung nach einer Sperrung entspricht der Identifizierung und Authentifizierung bei der initialen Registrierung.

3.4. Identifikation und Authentisierung bei Zertifikatsrückruf

Sachsen PKI Zertifikatsnehmer können die eigenen Zertifikate bzw. Zertifikate, für die als Service – verantwortliche Stelle im Auftrag gehandelt wird, zur Sperrung beantragen bzw. unmittelbar suspendieren.

4. Betriebliche Anforderungen an den Zertifikatslebenszyklus

Die Sachsen PKI dient der Ausgabe und Verwaltung Zertifikaten für Maschinen und Nutzer.

Zertifikatsantrag auf Nicht-Domänenmaschinen und Web Servern:

Die Erst-Beantragung und die Verlängerung eines Maschinenzertifikats für Web Server und Nicht-Domänenmaschinen erfolgt kontrolliert durch den zentralen Sachsen PKI Betrieb in Zusammenarbeit mit den entsprechenden Service – verantwortlichen Administratoren.

Zertifikatsantrag auf Domänenmaschinen:

Die Erst-Beantragung und die Verlängerung eines Maschinenzertifikats für Sachsen PKI Domänenmaschinen erfolgt teilautomatisiert über Gruppenrichtlinien. Dies bezieht sich auf alle Domänenmaschinen mit einem validen Maschinenkonto in der angeschlossenen Domäne. Eine Unterscheidung erfolgt anhand der Rolle der Maschine. Domänencontrollern werden hierbei angepasste Zertifikate zur Verfügung gestellt.

Nutzung von Sachsen PKI Maschinenzertifikaten:

Die Nutzung von Maschinenzertifikaten dient primär der Authentifizierung von Maschinen.

Folgende technische Rahmenbedingungen sind hervorzuheben:

- Eine CRL Überprüfung von Maschinen ist nicht flächendeckend möglich bzw. kann nicht flächendeckend gewährleistet werden, ist jedoch wo immer möglich und technisch mit vertretbarem Aufwand realisierbar erforderlich. Eine weitere mögliche Prüfung der eingesetzten Zertifikate ist gleichermaßen auf Applikationsebene durchzuführen.
- Zugehörige CRLs und CA-Zertifikate sind intern als auch extern über die in den eingesetzten Zertifikaten konfigurierten Attribute veröffentlicht bzw. erreichbar.

Weitergehende Informationen zum Einsatzbereich der von der Sachsen PKI ausgegebenen Zertifikate können bei Bedarf von dem zuständigen CA-Administrator erfragt oder der Webseite entnommen werden.

Nutzung von Sachsen PKI Benutzerzertifikaten:

Aktuell nicht zutreffend. Der Einsatz von Benutzerzertifikaten ist ab einem späteren Zeitpunkt geplant.

4.1. Zertifikatsantrag

4.1.1. Antragsberechtigt für ein Zertifikat

Antragsberechtigt für ein Zertifikat aus der Sachsen PKI sind:

- vom Freistaat Sachen bzw. dem beauftragten Dienstleistungsunternehmen und angeschlossenen Ressorts innerhalb des Freistaats betriebene Maschinen/Computer.
  - Maschinen, die in den angeschlossenen Domänen integriert sind.
  - Maschinen, die nicht in angeschlossenen Domänen integriert sind.
- Personen
  - die Mitarbeiter des Freistaates Sachsen sind und
  - ein valides AD Benutzerkonto in einer angeschlossenen Domäne besitzen und
  - zur Erfüllung ihrer Dienstpflichten ein Zertifikat benötigen.

4.1.2. Ausgabeprozess und Verantwortlichkeiten

Die Ausgabe von Zertifikaten erfolgt durch die zuständigen Sachsen PKI Issuing CAs der einzelnen Organisationseinheiten und / oder Ressorts. Die Verantwortlichkeit für den Ausgabeprozess obliegt dem Zertifikatsmanager.

4.2. Prozess für die Antragsbearbeitung

Wie auch beim Zertifikatsantrag ist die Antragsbearbeitung von teilautomatisch und manuell beantragten Maschinenzertifikaten ein kontrollierter Prozess gesteuert durch die für den Betrieb zuständige Organisationseinheit bzw. implementierte Automatismen.

Bei Maschinenzertifikaten für Domänen - integrierte Systeme stellt die Antragsbearbeitung einen teilautomatischen Prozess innerhalb der implementierten PKI und angeschlossener Systeme dar.

Bei Maschinenzertifikaten für nicht Domänen – integrierte Systeme stellt die Antragsbearbeitung einen manuellen Prozess der Beantragung durch die Service- verantwortliche Stelle bzw. Administrator nach etablierten Richtlinien der Sachsen PKI, der Prüfung und Freigabe durch die für den Prozess zuständige zentrale Organisationseinheit und die Implementierung des jeweiligen Zertifikats durch die Service – verantwortliche natürliche Person bzw. den zuständigen Administrator dar.

4.2.1. Durchführung der Identifikation und Authentifizierung

Die Identifikation und Authentifizierung des Antragsstellers erfolgt auf Basis valider Domänenkonten. Dies gilt sowohl für Benutzerkonten von Administratoren, die als Service – verantwortliche Stelle für eine Maschine handeln, als auch für Maschinen der Sachsen PKI angeschlossenen Domänen. Bei der manuellen Antragsbearbeitung von Maschinenzertifikaten muss ein valides Benutzerkonto der Service – verantwortlichen Stelle zur Authentifizierung existieren.

4.2.2. Annahme oder Ablehnung von Zertifikatsanträgen

Die Annahme oder Ablehnung von Zertifikatsanträgen erfolgt auf Basis valider Domänenkonten in Verbindung mit der Einhaltung der definierten Rahmenparameter des anzuwendenden Zertifikatsprofils.

4.2.3. Bearbeitungsdauer von Zertifikatsanträgen

Die Bearbeitung von Zertifikatsanträgen erfolgt automatisiert oder teilautomatisiert.

Werden Zertifikatsanträge über das Zertifikatsportal (CAM) eingestellt, so erfolgt sofort eine automatisierte Prüfung. Sofern bei dieser Prüfung abschließend entschieden werden kann, wird der Zertifikatsantrag sofort genehmigt und das Zertifikat ausgeliefert. Anderenfalls wird der Zertifikatsantrag zu weiteren Entscheidung den Mitarbeitern der zuständigen RA Stelle übergeben. Die RA Stelle soll innerhalb von 3 Arbeitstagen die Bearbeitung abschließen. Eine Gewähr zur Einhaltung dieser Frist kann jedoch nicht übernommen werden.

4.3. Zertifikatsausgabe

Bei Maschinenzertifikaten für Domänen – integrierte Systeme stellt die Zertifikatsausgabe einen teilautomatischen Prozess dar.

Bei Maschinenzertifikaten für nicht Domänen – integrierte Systeme stellt die Zertifikatsausgabe eine manuellen Prozess dar.

4.3.1. Aktivitäten der CA bei Zertifikatsausgabe

Vor Ausgabe der Zertifikate an die Zertifikatsnehmer werden folgende Arbeitsschritte CA - seitig ausgeführt.

- Validierung der Zertifikatsanforderung für ein Benutzer- oder Maschinenzertifikat durch das CA Richtlinienmodul.
  - Bei teilautomatisierter Ausgabe von Maschinenzertifikaten erfolgt die Validierung durch das Standard CA Richtlinienmodul.
  - Bei manueller Ausgabe von Maschinenzertifikaten erfolgt die Validierung initial durch den Zertifikatsmanager der Zertifizierungsstelle und anschließend durch das Standard CA Richtlinienmodul.

4.3.2. Ausgabebenachrichtigung der Zertifikatsnehmer durch die CA

Der Antragsteller wird über das bereitstehende Zertifikat zur Annahme und Implementierung auf dem jeweiligen System benachrichtigt.

4.4. Zertifikatsannahme

Bei Maschinenzertifikaten von Domänenmaschinen stellt die Zertifikatsannahme einen teilautomatischen Prozess und damit eine direkte implizite verbindliche Akzeptanz der für die Sachsen PKI geltenden Regularien gem. vorliegender CP / CPS Dokumente durch den service-verantwortlichen Administrator dar.

Bei manuell beantragten Maschinenzertifikaten wird die Annahme des Zertifikats und damit die verbindliche Akzeptanz der für die Sachsen PKI geltenden Regularien gem. vorliegender CP / CPS Dokumente durch den Service – verantwortlichen Administrator durchgeführt.

4.4.1. Verfahren der Zertifikatsannahme

Bei Domänenmaschinen sind Antragssteller und Zertifikatsnehmer identisch. Die Zertifikatsannahme findet analog zur Antragsstellung durch die antragsstellende Maschine statt. Mit Berechtigung der Maschinen zur Antragstellung stimmt der service-verantwortlichen Administrator implizit der Zertifikatsannahme zu.

Bei manuell beantragten Maschinenzertifikaten erfolgt die Antragsstellung und gesicherte Kommunikation im Namen des Zertifikatsnehmers durch einen Antragssteller in der Rolle eines für die Maschine Service – verantwortlichen Administrators, aber nicht durch den Zertifikatsnehmer selbst. Antragssteller und Zertifikatsnehmer in Form der Maschine unterscheiden sich in den aktuell etablierten Prozessen. Der Antragssteller ist in der Regel der RA Mitarbeiter oder ein Service – verantwortlicher Administrator, wohingegen der Zertifikatsnehmer die Maschine selbst ist. Die Zertifikatsannahme findet wie auch schon bei der Antragsstellung durch den Antragssteller statt.

4.4.2. Publikation des Zertifikats

End-Entitäten Zertifikate werden in der aktuellen Implementierung der Sachsen PKI nicht veröffentlicht.

Die Publikation der Sachsen PKI CA Zertifikate und Sperrlisten für die Sachsen Root CA 02 und die Issuing CAs wird auf den PKI Web Servern und in das angeschlossene Active Directory durch die Infrastruktur ausgeführt.

4.4.3. Ausgabebenachrichtigung anderer Entitäten durch die CA

Eine Ausgabebenachrichtigung an andere Entitäten durch die Sachsen PKI findet nicht statt.

4.5. Schlüsselpaar- und Zertifikatsverwendung

Grundsätzlich ist der Gebrauch des Schlüsselpaares zum Zwecke der Authentifizierung und / oder Verschlüsselung und / oder Signierung vorzusehen.

4.5.1. Nutzung des privaten Schlüssels und Zertifikats durch den Zertifikatsnehmer

Die Nutzung der Zertifikate durch den Zertifikatsnehmer hat den Sachsen PKI Zertifikatsrichtlinien zu folgen. Im Abschnitt 1.4. Anwendungsbereich von Zertifikaten sind die zulässigen und unzulässigen Anwendungen der Schlüssel bzw. Zertifikate festgelegt. Es sind weiterhin bei jeglicher Nutzung des privaten Schlüssels die in der Zertifikatsrichtlinie definierten Pflichten und Rahmenbedingungen zu erfüllen.

4.5.2. Nutzung der Zertifikate durch vertrauende Parteien

Die Nutzung der Zertifikate durch vertrauende Parteien hat den zugewiesenen Zertifikatsrichtlinien der jeweiligen Organisation und zwingend denen der Sachsen PKI zu folgen. Eine mögliche Kollision bestehender Richtlinien unterschiedlicher Organisationen ist vor der Beantragung von Zertifikaten der Sachsen PKI zu prüfen und aufzulösen. Die Beantragung von Zertifikaten der Sachsen PKI für jegliche Anwendungsfälle bedingt die vorherige Zustimmung zu den bestehenden Richtlinien und Regularien der Sachsen PKI – implizit oder explizit.

4.6. Zertifikatserneuerung

In Rahmen der Sachsen PKI findet die Zertifikatserneuerung ausschließlich mit Schlüsselwechsel statt. Eine Zertifikatserneuerung bei gleichem Schlüsselpaar, sprich ohne Schlüsselwechsel, ist nicht vorgesehen.

4.6.1. Zertifikatserneuerung mit Schlüsselwechsel

In Rahmen der Sachsen PKI findet die Zertifikatserneuerung ausschließlich mit Schlüsselwechsel statt. Technisch betrachtet handelt es sich um die Ersetzung eines Zertifikates durch ein Zertifikat mit neuer Gültigkeitsdauer für ein neues Schlüsselpaar mit sonst unveränderten Zertifikatsinhalten.

4.6.2. Umstände für eine Zertifikatserneuerung mit Schlüsselwechsel

Die Zertifikatserneuerung mit Schlüsselwechsel kann beantragt werden, wenn eine der folgenden Voraussetzungen erfüllt ist:

- die Gültigkeitsdauer des aktuellen Zertifikats ist abgelaufen oder steht kurz vor Ablauf,
- das aktuelle Zertifikat wurde gesperrt,
- die im Zertifikat enthaltenen Daten sind nicht mehr korrekt,
- der alte Schlüssel kann oder darf nicht mehr verwendet werden, weil er (möglicherweise) kompromittiert wurde,
- die Gültigkeitsdauer des aktuellen Zertifikats, die aktuelle Schlüssellänge bzw. die verwendeten Algorithmen bieten keine ausreichende Sicherheit mehr,
- das Zertifikat kann technisch nicht mehr genutzt werden (Verlust des privaten Schlüssels oder kein Zugriff auf privaten Schlüssel etc.).

4.6.3. Antragsberechtigte für eine Zertifikatserneuerung mit Schlüsselwechsel

Sind alle Zertifikatsnehmer, denen ein gültiges Sachsen PKI Zertifikat durch die Sachsen PKI zugewiesen wurde.

4.6.4. Durchführen einer Zertifikatserneuerung mit Schlüsselwechsel

Der Prozess erfolgt analog der Erst-Antragsstellung. Die Sachsen PKI führt die Zertifikatserneuerung mit Schlüsselwechsel teilautomatisiert für Domänen – integrierte Systeme aus. Im Falle von manuell auszurollenden Maschinenzertifikaten erfolgt der Erneuerungsprozess kontrolliert analog zum initialen Beantragungsprozess.

4.6.5. Erneuerungsbenachrichtigung für den Zertifikatsnehmer

Eine Erneuerungsbenachrichtigung ist bei teilautomatisiert ausgegebenen Zertifikaten für Maschinen nicht erforderlich. Vor Ablauf der Zertifikatsgültigkeitsdauer wird ein teilautomatisierter Erneuerungsprozess durch die Sachsen PKI angestoßen.

Bei manuell ausgestellten Zertifikaten findet keine Erneuerungsbenachrichtigung durch die Sachsen PKI statt. Der dem System zugeordnete Service – verantwortliche Administrator ist für die Überwachung der Gültigkeit und eine entsprechend frühzeitige Erneuerung des Zertifikats zur Aufrechterhaltung des konsumierenden Dienstes selbst verantwortlich.

4.6.6. Verfahren zur Annahme der Zertifikatserneuerung mit Schlüsselwechsel

Bei Domänen – integrierten Systemen sind Antragssteller und Zertifikatsnehmer identisch. Die Zertifikatsannahme bei Erneuerung findet wie auch schon bei der Antragsstellung durch die antragsstellende Maschine statt.

Bei manuell beantragten Maschinenzertifikaten erfolgt die Antragsstellung und gesicherte Kommunikation in Namen des Zertifikatsnehmers durch einen Antragssteller in Form des Service - verantwortlichen Administrators, aber nicht durch den Zertifikatsnehmer selbst. Antragssteller und Zertifikatsnehmer unterscheiden sich. Der Antragssteller ist in der Regel der RA Mitarbeiter oder ein zuständiger Administrator, wohingegen der Zertifikatsnehmer die Maschine selbst ist. Die Zertifikatsannahme bei Erneuerung findet wie auch schon bei der Antragsstellung durch Antragssteller statt.

Wenn eine erfolgreiche Authentifizierung durch den Zertifikatsnehmer (Maschine oder Benutzer) mittels des erneuerten Zertifikats ausgeführt werden kann, gilt das erneuerte Zertifikat als durch den Zertifikatsnehmer angenommen.

4.6.7. Publikation des erneuerten Zertifikats durch die CA

Es gelten die gleichen Regelungen zu Abschnitt 4.4.2. Publikation des Zertifikats.

4.6.8. Erneuerungsbenachrichtigung anderer Entitäten durch die CA

Eine Ausgabebenachrichtigung an andere Entitäten durch die Sachsen PKI findet nicht statt.

4.7. Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

In Rahmen der Sachsen PKI findet die Zertifikatserneuerung ausschließlich mit Schlüsselwechsel statt. Eine Anpassung der Zertifikatsinhalte (Datenanpassung) ist nicht vorgesehen.

4.8. Zertifikatssperrung und -suspendierung

In der aktuellen Implementierung der Sachsen PKI ist sowohl eine Zertifikatssperrung als auch eine Zertifikatssuspendierung vorgesehen.

4.8.1. Umstände für die Sperrung

Ein Zertifikat ist in den folgenden Fällen zu sperren:

- Wenn der berechtigte Verdacht besteht, dass der private Schlüssel, der zum öffentlichen Schlüssel im Zertifikat korrespondiert, kompromittiert wurde, d.h. dass ein Unbefugter den privaten Schlüssel nutzen kann.
- Wenn der berechtigte Verdacht besteht, dass die für die Erzeugung und Anwendung des privaten Schlüssels, der zum öffentlichen Schlüssel im Zertifikat korrespondiert, eingesetzten Algorithmen, Parameter und Geräte die Fälschungssicherheit der erzeugten Signaturen nicht mehr gewährleisten.
- Wenn das Zertifikat technisch nicht mehr nutzbar ist, z.B. der Zugriff auf das Schlüsselmaterial nicht mehr besteht.
- Wenn zu dem Zertifikat, eine Zertifikatserneuerung mit Schlüsselwechsel beantragt wurde.
- Wenn die Sachsen PKI bzw. eine untergeordnete CA ihre Zertifizierungsdienste eingestellt hat. In diesem Fall werden sämtliche von den Zertifizierungsdiensten in diesem Zweig ausgestellten Zertifikate gesperrt.
- Die Zertifikate sind zu sperren, wenn der Zertifikatseigentümer die Voraussetzungen für die Verwendung des Zertifikates nicht mehr erfüllt, z.B. weil die betreffende Maschine außer Dienst gestellt wird oder gegen die bestehende Zertifikatsrichtlinie verstoßen wird.
- Zertifikate werden automatisch gesperrt, wenn die korrespondierenden AD-Objekte blockiert oder gelöscht werden.

4.8.2. Antragsberechtigte für eine Sperrung

Folgende Personenkreise und Instanzen sind berechtigt Zertifikate zu sperren:

- die Sperrung von Zertifikaten kann durch
  - den Zertifikatsnehmer selbst (Zertifikatsinhaber/-nehmer)
  - seinen dienstlichen Vertreter
  - seinen Vorgesetzten oder

- durch den Sachsen PKI Registrierungsstellenmitarbeiter veranlasst werden.
- Die Sperrung von CA Zertifikaten kann durch die Aufsicht der Sachsen PKI Zertifizierungsstellen veranlasst werden.

4.8.3. Durchführung einer Zertifikatssperrung

Der Service-verantwortliche Administrator sperrt unter Angabe des Sperrgrundes von ihm beantragte Zertifikate über das Zertifikatsportal (CAM) und veröffentlicht anschließend eine neue Sperrliste.

Eine Ausnahme bildet die sofortige Sperrung, die durch eine E-Mail veranlasst werden kann. Zertifikatsnummer und Sperrgrund müssen enthalten sein. Es erfolgt die initiale Identifizierung des zuständigen Service – verantwortlichen Administrators durch seine Absender-E-Mail Adresse und eine Rückfrage. Stellvertretend kann auch ein Vorgesetzter des Mitarbeiters diesen Antrag stellen. Die Zertifikatssperrung und Sperrlistenveröffentlichung wird durch die der Sachsen PKI vorgeschaltete Registrierungsstelle bzw. der mit dem Betrieb der CA beauftragte CA-Administrator durchgeführt.

4.8.4. Meldefrist von Sperranträgen für Zertifikatsnehmer

Es sind keine vorgeschriebenen Fristen festgelegt. Grundsätzlich soll eine Meldung von Sperranträgen direkt und möglichst umgehend erfolgen.

4.8.5. Bearbeitungsdauer von Sperranträgen durch die CA

Es ist keine festgeschriebene Bearbeitungsdauer von Sperranträgen durch die CA spezifiziert. Es wird eine umgehende und aus Gesichtspunkten des notwendigen Aufwands vertretbare zeitnahe Sperrung angestrebt.

4.8.6. Prüfung des Zertifikatsstatus durch vertrauende Parteien

Eine Überprüfung des Zertifikatsstatus durch vertrauende Parteien wird empfohlen. Der Sperrstatus von Sachsen PKI Zertifikaten und von Sachsen PKI Zertifizierungsstellenzertifikaten kann über die entsprechenden Sperrlisten oder ggf. über OCSP-Anfragen geprüft werden. Die aktuellen Zertifikatssperrlisten können durch die in den Zertifikat enthaltenen CDP (CRL Distribution Points) Attributen intern als auch extern heruntergeladen werden.

4.8.7. Ausstellungszeiträume für CRLs

Die Ausstellungszeiträume sind für die Sachsen PKI im Abschnitt 1.3.1. Zertifizierungsstellen aufgelistet.

4.8.8. Maximale Latenz von CRLs

Die CRLs stehen sofort nach Veröffentlichung (und Replikation) im angeschlossenen Active Directory und auf den Sachsen PKI Web-Servern zur Verfügung. Eine durch Systeme der Sachsen PKI verursachte bzw. zu verantwortende Latenzzeit bei der Erstellung und Verfügbarkeit von CRLs ist daher nicht zu erwarten, kann jedoch durch weitere möglicherweise beteiligte externe Systeme nicht ausgeschlossen werden.

4.8.9. Online Sperrung und Statusprüfung von Zertifikaten

Eine Online Statusprüfung mittels OCSP (Online Certificate Status Protocol) für die Sachsen PKI wird eingesetzt (Online-Abfrage von Sperrlisteneinträgen).

4.8.10. Anforderung für die Online Prüfung des Sperrstatus

Die implementierte Clientbasis muss die Nutzung von OCSP unterstützen.

4.8.11. Weitere Arten zur Bekanntmachung des Zertifikatsstatus

Es sind keine weiteren Arten zur Bekanntmachung des Zertifikatsstatus vorgesehen. Die Sperrlisten werden auf Web-Servern und im Active Directory veröffentlicht, welche im Zertifikat über die CDP Einträge bekannt gemacht werden.

4.8.12. Spezielle Maßnahmen bei Schlüsselkompromittierung

Bei einem Hinweis einer Schlüsselkompromittierung wird eine sofortige Untersuchung durchgeführt. Sollte sich der Kompromittierungsverdacht als stichhaltig erweisen, so werden umgehend alle für die Sperrung notwendigen Maßnahmen ergriffen.

4.9. Auskunftsdienste für den Zertifikatsstatus

Die Sachsen PKI betreibt einen Auskunftsdienst über den Zertifikatsstatus. Dieser Auskunftsdienst ist webbasiert und über eine HTTP URL als auch bei internem Aufruf per LDAP aus dem angeschlossenen Active Directory Verzeichnisdienst erreichbar. Es werden die CRLs (Zertifikatssperrlisten) veröffentlicht:

- Die Statusinformationen zu Maschinenzertifikaten werden in der CRL aufgeführt, welche durch die Sachsen PKI Issuing CAs ausgegeben und veröffentlicht werden.
- Die Statusinformationen zu Zertifikaten der Zertifizierungsstellen werden in der CRL aufgeführt, welche durch die Sachsen Root CA 02 ausgegeben und veröffentlicht wird.

Für jede der in der Sachsen PKI eingesetzten CAs werden separate CRLs (Sperrlisten) veröffentlicht.

Zusätzlich wird ein OCSP-Dienst zur Onlineabfrage von Sperrlisteneinträgen angeboten.

4.9.1. Betriebliche Ausprägung

Der Auskunftsdienst basiert auf einem LDAP Verzeichnisdienst in Form des Active Directory. Zusätzlich werden die CRLs auf Web-Servern bereitgestellt.

Darüber hinaus wird ein OCSP-Dienst im Internet und Intranet bereitgestellt.

Die URLs sind in Abschnitt 2.2. Publikation von Zertifizierungsinformationen gelistet. Die CRLs und zu sperrende Zertifikate müssen von der gleichen Zertifizierungsstelle ausgegeben worden sein. Eine Unterstützung von „indirekten CRLs“ ist in der jetzigen Implementierung nicht gegeben.

Das ausgegebene CRL Profil ist zum RFC 5280 konform und entspricht dem X.509 Version 2 Standard.

4.9.2. Verfügbarkeit des Auskunftsdienstes

Die Verfügbarkeit der Sachsen PKI Web-Server, der Sachsen PKI angeschlossenen Active Directory Verzeichnisdienste und aller an der PKI beteiligten Systeme ist für einen 7 x 24h Betrieb ausgelegt. Die Verfügbarkeit entspricht den mit dem Vertragspartner bestehenden vereinbarten Regelungen (99,5 % Verfügbarkeit im gleitenden 3-Monatsmittel).

4.10. Schlüsselhinterlegung und -wiederherstellung

Eine Schlüsselhinterlegung und –wiederherstellung wird in Rahmen der aktuellen Implementierung der Sachsen PKI nicht umgesetzt.

4.10.1. Richtlinien und Praktiken zur Schlüsselhinterlegung und -Wiederherstellung

Nicht zutreffend.

4.10.2. Richtlinien und Praktiken zur Hinterlegung und Wiederherstellung von Sitzungsschlüsseln (symmetrische Schlüssel)

Nicht zutreffend.

5. Einrichtungen, Sicherheitsmanagement, organisatorische und betriebliche Sicherheitsmaßnahmen

5.1. Physikalische- und Umgebungssicherheit

Die infrastrukturellen Sicherheitsmaßnahmen der Sachsen PKI sind in den Rechenzentrumsbetrieb des Freistaats Sachsen bzw. im Auftrag handelnder Partnerunternehmen eingebunden. Folgende Vorkehrungen und physikalische Schutzmaßnahmen sind integraler Bestandteil der Rechenzentren, betrieben durch den Freistaat Sachen bzw. im Auftrag handelnder Partnerunternehmen.

5.1.1. Lage und Konstruktion

Die Systeme der Sachsen PKI befinden sich in den Räumlichkeiten des Rechenzentrumspartners „Deutsche Telekom“. Die Räume bieten hinsichtlich der physikalischen Sicherheitsmaßnahmen einen ausreichenden Schutz, der dem erforderlichen Sicherheitsniveau angemessen ist.

5.1.2. Zutrittskontrolle

Die Betriebsräume der Zertifizierungsstellen sind durch geeignete technische und infrastrukturelle Maßnahmen gesichert. Ein Zutritt zu den Betriebsräumen der Zertifizierungsstelle wird nur Mitarbeitern gestattet, die die entsprechende Freigabestufe besitzen. Der Zutritt durch betriebsfremde Personen wird durch eine Besucherregelung festgelegt.

5.1.3. Stromversorgung und Klimatisierung

Die Installation zur Stromversorgung entspricht den erforderlichen Normen, eine Klimatisierung der Räume für die technische Infrastruktur ist vorhanden.

5.1.4. Wasserschäden

Die Räume für die technische Infrastruktur verfügen über einen angemessenen Schutz vor Wasserschäden.

5.1.5. Prävention und Schutz vor Feuer

Die bestehenden Brandschutzvorschriften werden eingehalten, Handfeuerlöscher sind in ausreichender Anzahl vorhanden.

5.1.6. Datenträger

Es werden folgende Datenträger verwendet:

- Papier
- DVD/CD-Datenträger
- USB-Speichermodule
- Hardwaretoken/Smartcards

Datenträger werden in verschlossenen Schränken aufbewahrt. Datenträger mit sensiblen Daten werden in Tresoren aufbewahrt.

5.1.7. Abfall Entsorgung

Nicht mehr benötigte Informationen auf elektronischen Datenträgern und auf Papier werden sachgemäß vernichtet.

5.1.8. Off-site Backup

Eine Off-Site Sicherung erfolgt für alle CAs.

5.2. Organisatorische Sicherheitskontrollen

5.2.1. Sicherheitskritische Rollen

Sicherheitskritische Aufgaben werden für den Betrieb der Sachsen PKI in Rollen zusammengefasst. Ein PKI Rollenkonzept ist verfügbar und wird für den organisatorischen Prozess und auch für den HSM (Hardware Security Module) Betrieb umgesetzt.

5.2.2. Zugewiesene Zahl von Personen bei sicherheitskritischen Aufgaben

Das Vier- bzw. n-Augen-Prinzip gilt bei folgenden Operationen:

- Wiederherstellen des Schlüsselmaterials der Sachsen PKI Zertifizierungsstellen
- Wiederherstellen der Sachsen PKI Zertifizierungsstellen
- Zugriff auf die Hardware Security Module der Sachsen PKI Zertifizierungsstellen

5.2.3. Identifikation und Authentifikation der Rollen

Die Identifikation und Authentifizierung der Benutzer erfolgt beim Zutritt zu sicherheitsrelevanten Räumen und beim Zugriff auf sicherheitsrelevante Systeme mit Hilfe von Smartcards, Hardware Tokens und/oder Benutzername und Passwort.

Bei besonders sicherheitskritischen Operationen, wie die Verwaltung bzw. Verwendung von Zertifizierungsstellenschlüsseln kommt das Vier- bzw. n-Augen-Prinzip zum Einsatz.

5.2.4. Trennung von Rollen und Aufgaben

Das Rollenkonzept regelt auch, welche Zuordnungen von Personen zu Rollen sich gegenseitig ausschließen. Dabei liegen die folgenden Grundregeln zugrunde:

- Leitende Rollen dürfen keine operativen oder administrativen Aufgaben übernehmen
- Kontrollierende und beratende Rollen dürfen keine operativen oder administrativen Aufgaben übernehmen
- Administrative Rollen dürfen keine operativen Aufgaben übernehmen

Daneben gelten weitere Ausschlüsse zur Trennung der folgenden sicherheitskritischen Verantwortlichkeiten:

- Einhaltung der Sicherheitsvorschriften und die Prüfung durch Audits
- Zutritt zu den Räumlichkeiten der Zertifizierungsstellen und Zugriff auf die internen Systeme

Die entsprechende Rollentrennung ist in der Sachsen PKI technisch und organisatorisch untersetzt (4- oder 6-Augen-Prinzip, aktivierte Rollentrennung in der CA-Software, getrennte Token).

5.3. Sicherheitsmaßnahmen für das Personal

Der Freistaat Sachsen bzw. der mit dem Betrieb beauftragte Dienstleistungspartner stellt im Umfeld der Sachsen PKI erfahrenes Personal zur Verfügung. Notwendige Qualifikation, Wissenstand und Erfahrungswerte des Personals sind für den sicheren PKI Regelbetrieb vorhanden.

5.3.1. Anforderung an Qualifikation, Erfahrung und Freigabestufe

Das zuständige Personal verfügt über die erforderlichen spezifischen Kenntnisse und Erfahrungen aus dem Bereich der X.509 PKI. Ebenso sind grundlegende IT Kenntnisse vorhanden um auch systemnahe Operationen auszuführen.

5.3.2. Prozess zur Sicherheitsüberprüfung von Mitarbeitern

Es gelten die allgemeinen Personaleinstellungsrichtlinien des Freistaats Sachsen bzw. der mit dem Betrieb beauftragte Dienstleistungspartner. Die Sicherheitsstufe „Ü1“ ist als Mindestanforderung für das gesamte Sachsen PKI Personal zu gewährleisten.

5.3.3. Trainingsanforderung

Das für den Zertifizierungsdienst eingesetzte Personal wird vor Aufnahme der Tätigkeit ausreichend geschult. Das Training beinhaltet auch eine Sensibilisierung der Mitarbeiter hinsichtlich der Sicherheitsrelevanz ihrer Arbeit und potenzieller Bedrohungen.

5.3.4. Trainingsfrequenz

Die Frequenz der Trainings orientiert sich an den Anforderungen der Sachsen PKI. Trainings werden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und Sicherheitstechnik als auch bei signifikanten Änderungen der bestehenden Implementierung durchgeführt.

5.3.5. Frequenz und Abfolge von Job Rotation

Eine Job Rotation ist nicht vorgesehen.

5.3.6. Sanktionen bei unzulässigen Handlungen

Die allgemeinen Sanktionsmöglichkeiten des Freistaat Sachsen bzw. der mit dem Betrieb beauftragte Dienstleistungspartner werden bei unzulässigen Handlungen angewandt.

5.3.7. Vertragsbedingungen für das Personal

Das Sachsen PKI Betriebspersonal verpflichtet sich auf die Einhaltung von Anweisungen und gesetzlichen Vorschriften. Diese beinhalten insbesondere eine Verpflichtung, personenbezogene Daten vertraulich und im Rahmen bestehender Dienstanweisungen zu behandeln.

5.3.8. An das Personal ausgehändigte Dokumente

Folgende Dokumente werden dem Sachsen PKI Personal zum ordnungsgemäßen Betrieb der PKI zur Verfügung gestellt:

- Zertifikatsrichtlinie / Certificate Policy (CP) und Erklärung zum Zertifizierungsbetrieb / Certification Practice Statement (CPS)
- Betriebskonzept und Sicherheitskonzept der Sachsen PKI CAs und beteiligten Systeme
- Handlungsanweisungen
- Betriebshandbücher der Systeme und Software

5.4. Überwachung von sicherheitskritischen Ereignissen

5.4.1. Protokollierte Ereignisse

Zu jedem Ereignis werden folgenden Daten erfasst:

- Zeitpunkt (Datum und Uhrzeit)
- Log ID des Eintrags
- Art des Ereignisses
- Ursprung des Ereignisses

Die folgenden Ereignisse werden elektronisch protokolliert:

- Ereignisse im Lebenszyklus von Zertifikaten und Schlüsselpaaren:
  - Sicherung und Wiederherstellung der CA-Datenbasis
  - Änderung der CA-Konfiguration
  - Änderungen der CA-Sicherheitseinstellungen
  - Verwaltung von Zertifizierungsanforderungen
  - Speicherung und Wiederherstellung von Schlüsseln
  - Start und Stop der Zertifikatsdienste
  - Ausstellung von Zertifikaten
  - Sperrungen
  - Erstellung von Sperrlisten
- Ereignisse im Lebenszyklus der HSMs:
  - Initialisierung eines HSM
  - Änderung der Konfiguration eines HSM
  - An- und Abmeldung an einem HSM
  - Generierung von Schlüsseln in einem HSM
  - Backup und Wiederherstellung von Schlüsseln in einem HSM
  - Löschen von Schlüsseln in einem HSM
- Systemereignisse und Fehlermeldungen der sicherheitskritischen Systeme:
  - Versuche zur An- und Abmeldung
  - Vergabe, Entzug und Verwendung von Zugriffsberechtigungen
  - Richtlinienänderung
- Ereignisse der Zutrittskontrollanlagen:
  - Betreten und Verlassen von gesicherten Räumen
  - Fehlgeschlagene Zutrittsversuche und Alarme
  - Vergabe und Entzug von Zutrittsberechtigungen
  - Beantragung, Ausgabe und Sperrung von Zutrittskarten

5.4.2. Überprüfungshäufigkeit von Log-Daten

Eine Überprüfung der Log-Daten findet in regelmäßigen Abständen statt. Bei Verdacht auf Unregelmäßigkeiten wird eine umgehende Prüfung veranlasst.

5.4.3. Aufbewahrungsfristen von Audit Log-Daten

Sicherheitsrelevante Protokolldaten werden entsprechend den Regelungen des SVN aufbewahrt.

5.4.4. Schutzmaßnahmen von Audit Log-Daten

Elektronische Log-Dateien werden mit Mitteln des Betriebssystems gegen Zugriff, Löschung und Manipulation geschützt und sind nur den System- und Netzwerkadministratoren gem. der Dienstanweisungen zugänglich.

5.4.5. Audit Log-Daten Backup-Verfahren

Die Protokolldaten werden zusammen mit anderen relevanten Daten der Sachsen PKI einem regelmäßigen Backup unterzogen. Protokolle auf Papier werden in verschließbaren Schränken verwahrt.

5.4.6. Audit Collection System (Protokollierungssystem intern oder extern)

Alle Protokoll-Dateien werden regelmäßig gesichert.

5.4.7. Benachrichtigung bei Auslösen eines sicherheitskritischen Ereignisses

Eine Benachrichtigung des PKI Bedienerpersonals über E-Mail findet bei Auftreten von sicherheitskritischen Ereignissen statt.

5.4.8. Schwachstellenanalyse

Eine Schwachstellenanalyse der Sachsen PKI durch den Freistaat Sachsen bzw. ein vom ihm beauftragtes Unternehmen ist vorgesehen.

5.5. Archivierung von Protokolldaten

Der Freistaat Sachsen bzw. der mit dem Betrieb beauftragte Dienstleistungspartner archiviert im Rahmen des PKI Betriebes die notwendigen Protokolldaten.

5.5.1. Archivierte Protokolldatentypen

Archiviert werden Daten, die für den Zertifizierungsprozess relevant sind:

- Zertifikatsanträge, diese enthalten persönliche Daten des Zertifikatnehmers
- Sperranträge für Verschlüsselungs/Signatur-Zertifikate und für Zertifizierungsstellen-Zertifikate
- Vor einer Modifikation eines Systems gesicherte Systemdaten
- Datensicherungen der Produktivsysteme
- Dokumentation der personellen Sicherheitsmaßnahmen (z.B. Dienstpläne, Dokumentation der Sicherheitsüberprüfungen)

- Dokumentationen von Prozeduren und Systemen (z.B. Handlungsanweisungen, Notfallpläne, Systemhandbücher)
- Protokolle von sicherheitsrelevanten internen Prozeduren und Prozesse:
  - Prozeduren der Schlüsselzeremonie
  - Prozeduren bei Installation und Konfiguration der Zertifizierungsstellen
  - Prozeduren bei Installation und Konfiguration der PKI
  - Notfallprozeduren
  - Change-Management-Prozeduren
  - Zugang zu den geschützten Räumlichkeiten durch externes Personal.
  - Prüfung, Installation und Administration von HSMs
  - Ausgabe von Zutrittskarten zu geschützten Räumlichkeiten
  - Änderung, Kenntnisnahme oder Übergabe von PINs und Passwörtern für HSMs
  - Änderungen in den Zuweisungen von Rollen

5.5.2. Archivierungsfristen

Zu archivierende Daten werden mindestens 2 Jahre aufbewahrt.

5.5.3. Schutzmaßnahmen für das Archiv

Es wird durch geeignete Maßnahmen sichergestellt, dass die Daten nicht verändert oder gelöscht werden können. Sind in den Archiven personenbezogene Daten enthalten, wird darüber hinaus sichergestellt, dass die Daten nicht unbefugt gelesen oder kopiert werden können.

Die Schutzmaßnahmen für elektronische Datenträger entsprechen den für den Rechenzentrums-Betrieb des Freistaat Sachsen bzw. des mit dem Betrieb beauftragten Dienstleistungspartners vorgesehenen Prozessen:

- Das Archiv befindet sich in einem zutrittsgeschützten Bereich.
- Die Archive sind durch Klimaanlagen und Vorrichtungen zum Brandschutz vor Umwelteinflüssen geschützt.
- Der Freistaat Sachsen bzw. der mit dem Betrieb beauftragte Dienstleistungspartner ist verantwortlich für die Übertragung der archivierten elektronischen Daten im Fall einer Technologieablösung auf aktuelle Datenträgertypen.

5.5.4. Backup-Verfahren für das Archiv

Es erfolgt kein Backup des Archivs.

5.5.5. Zeitstempelanforderungen für archivierte Daten

Audit Logs, protokollierte Ereignisse, archivierte Daten, Zertifikate, Zertifikatssperrlisten und andere Eintragungen enthalten jeweils eine eindeutige Zeit- und Datumsangabe. Datums- und Zeitangaben von Online-Systemen werden in regelmäßigen Abständen gegen eine vertrauenswürdige Zeitquelle synchronisiert.

5.5.6. Archivierungssystem (intern oder extern)

Ein Archivierungssystem wird in Rahmen der Sachsen PKI nicht eingesetzt.

5.6. Schlüsselwechsel der Zertifizierungsstellen

Bei einem Schlüsselwechsel der Sachsen Root CA 02 wird das aktuelle CA Zertifikat gelöscht und ein neues selbst-signiertes Zertifikat ausgestellt und veröffentlicht. Eine Sperrung des selbst-signierenden Root CA Zertifikats ist technisch auf der CA Seite nicht machbar.

Bei einem Schlüsselwechsel der Ressort-CA werden die aktuellen Issuing CA Zertifikate von der Sachsen Root CA 02 gesperrt und neue Zertifikate ausgestellt und veröffentlicht. Die Beantragung selbst erfolgt auf den Issuing CAs.

5.7. Kompromittierung und Wiederanlauf nach Katastrophen

5.7.1. Prozeduren bei Sicherheitsvorfällen und Kompromittierung

Es existieren Notfallpläne des Freistaats Sachsen bzw. des mit dem Betrieb beauftragten Dienstleistungspartners, in denen die Prozesse, Prozeduren und Verantwortlichkeiten bei Notfällen und Katastrophen geregelt sind. Zielsetzung dieser Notfall -Prozeduren ist die Minimierung von Ausfällen der Zertifizierungsdienstleistungen bei gleichzeitiger Aufrechterhaltung der Sicherheit. Die Notfall-Prozeduren sehen bei Sicherheitsvorfällen insbesondere die folgenden Maßnahmen vor:

- Analyse und Bewertung der Funktionseinschränkung und Sicherheitsprobleme der betroffenen Dienste und Systeme der Zertifizierungsstelle,
- Festlegung von Sofortmaßnahmen, die den Funktionseinschränkungen und Sicherheitsproblemen entgegenwirken,
- Regelung der Verantwortlichkeiten und Rollen,
- Falls erforderlich, Benachrichtigung betroffener Stellen und Personen, z.B. der Zertifikatsnehmer, über die Problematik und gegebenenfalls notwendige Gegenmaßnahmen,
- Analyse und Dokumentation der Ursachen des Vorfalles,
- Gegebenenfalls Erstellung, Prüfung und Genehmigung eines Change Requests zur Modifikation der Systemkonfiguration mit dem Ziel, Vorfälle dieser Art in Zukunft zu verhindern. Überwachung der Umsetzung des Change Requests,
- Protokollierung der einzelnen Maßnahmen und Tätigkeiten.

5.7.2. Kompromittierung bei IT Ressourcen

Werden innerhalb der Zertifizierungsstelle fehlerhafte oder manipulierte Rechner, Software und/oder Daten festgestellt, die Auswirkungen auf die Prozesse der Zertifizierungsstelle haben,

- wird der Betrieb des entsprechenden IT-Systems unverzüglich eingestellt.
- Das IT-System wird auf einer Ersatzhardware unter Wiederherstellung der Software und der Daten aus der Datensicherung neu aufgesetzt, überprüft und in einem sicheren Zustand in Betrieb genommen.
- Anschließend wird das fehlerhafte oder modifizierte IT-System analysiert. Bei Verdacht einer vorsätzlichen Handlung werden gegebenenfalls rechtliche Schritte eingeleitet.
- Falls sich in einem Zertifikat fehlerhafte Angaben befinden, wird der Zertifikatnehmer unverzüglich informiert und das Zertifikat widerrufen.

5.7.3. Wiederanlauf bei Kompromittierung von privatem Schlüsselmaterial

Die Kompromittierung von privatem Schlüsselmaterial stellt einen ernstzunehmenden Zwischenfall dar und wird daher besonders gehandhabt.

- Bei Kompromittierung von privatem Schlüsselmaterial der Zertifizierungsstellen wird das jeweilige Zertifikat sofort gesperrt. Gleichzeitig werden alle mit Hilfe dieses Zertifikats ausgestellten Zertifikate gesperrt.
- Bei Kompromittierung von privatem Schlüsselmaterial des Sachsen PKI Zertifikats wird das jeweilige Zertifikat sofort gesperrt.
- Bei Kompromittierung von privatem Schlüsselmaterial der Maschinenzertifikate werden Zertifikate mit neuem Schlüsselmaterial ausgegeben. Eine Sperrung der kompromittierten Zertifikate wird ebenfalls durchgeführt.
- Sofern der Verdacht besteht, dass die für die Erzeugung und Anwendung des privaten Schlüssels eingesetzten Algorithmen, Parameter oder Geräte unsicher sind, wird eine entsprechende Untersuchung durchgeführt.
- Alle betroffenen Zertifikatsnehmer und vertrauende Parteien werden umgehend benachrichtigt.

Ein Wiederanlauf der betroffenen Komponenten darf nur dann erfolgen, wenn das kompromittierte Schlüsselmaterial durch ein einwandfreies Schlüsselmaterial ersetzt wurde und auch dieses in Rahmen des Anwendungsprofils tatsächlich genutzt wird.

5.7.4. Notfallbetrieb nach einem Katastrophenfall

Eine Wiederaufnahme des Zertifizierungsbetriebs nach einer Katastrophe bei Verlust ist Bestandteil der Notfallplanung und kann innerhalb kurzer Zeit erfolgen, sofern die Sicherheit der Zertifizierungsdienstleistung gegeben ist.

5.7.5. Einstellung des Betriebs der Zertifizierungs- und/oder Registrierungsstelle

Im Falle der Einstellung des Betriebes der Sachsen PKI Zertifizierungsstellen und eines Zweigs der Zertifizierungskette oder der Registrierungsstellen sind folgende Maßnahmen festgelegt:

- Alle Zertifikatsnehmer und die vertrauenden Parteien werden von der Einstellung des Zertifizierungsdienstes informiert. Eine zeitliche Frist wurde noch nicht festgelegt. Mindestfrist von zwei Monaten vor Einstellung wird angedacht.
- Alle Sachsen PKI Zertifikate, sowie die Zertifikate der Zertifizierungsstellen werden gesperrt.
- Alle privaten Schlüssel der Zertifizierungsstellen und der Zertifikate der Zertifikatsnehmer werden vernichtet.

6. Technische Sicherheitsmaßnahmen

6.1. Schlüsselpaarerzeugung und Installation

6.1.1. Schlüsselpaarerzeugung

Die Schlüsselerzeugung und die Auswahl der Crypto-Algorithmen für die Sachsen PKI erfolgt nach FIPS 140-2 Level 2 (Federal Information Processing Standards).

Die Generierung der Schlüsselpaare wird von Hard- und Softwarekomponenten ausgeführt und unterscheidet sich je nach Entität:

Schlüsselpaargenerierung für die Sachsen PKI Zertifizierungsstellen:

Alle Schlüsselpaare für die Sachsen PKI Zertifizierungsstellen werden durch das HSM (Hardware Security Modul) generiert. Die generierten CA Schlüssel werden auch durch das HSM kryptographisch geschützt. In jeglichen Prozess, der den Zugriff auf den privaten Schlüssel der Zertifizierungsstelle erforderlich macht, ist das HSM zwingend eingebunden. Die Sachsen PKI HSMs werden im FIPS 140-2 Level 2 Modus betrieben. Der Zugriff auf den privaten Schlüssel wird zusätzlich über ein Vier- bzw. n-Augen Prinzip durch eine starke Authentifizierung abgesichert.

Schlüsselpaargenerierung der Sachsen PKI Maschinen (Authentifikation):

Die Authentifzierungsschlüsselpaare werden selbst auf den beantragenden Maschinen generiert. Die Generierung des Schlüsselmaterials erfolgt in diesem Fall durch Softwarekomponenten. Die Software Krypto-Komponenten sind nach FIPS 140-2 Level 1 zertifiziert.

6.1.2. Auslieferung der privaten Schlüssel an Zertifikatsnehmer

Private Schlüssel der Sachsen PKI Zertifizierungsstellen:

In jeglichen Prozess, der den Zugriff auf den privaten Schlüssel der Zertifizierungsstelle erforderlich macht, ist das HSM zwingend eingebunden. Alle privaten CA Schlüssel liegen nur in einem von dem HSM gesicherten Umfeld vor.

Eine Auslieferung des privaten Schlüsselmaterials von CA Schlüsseln ist nicht notwendig, da die HSM für die Schlüsselerzeugung und als Absicherung für private Schlüssel dient.

Private Schlüssel der Sachsen PKI Maschinen (Authentifikation):

Die Authentifizierungsschlüsselpaare werden selbst auf den beantragenden Maschinen generiert.

Eine Auslieferung ist nur dann notwendig, wenn die Zielmaschine (Zertifikatsnehmer) nicht identisch ist mit der beantragenden Maschine. In diesem Fall erfolgt die Auslieferung des privaten Schlüssels an die Zielmaschine (Zertifikatsnehmer) über geeignete sichere Verfahren, wie PKCS#12. Sind Zielmaschine und beantragende Maschine identisch, so ist eine Auslieferung nicht notwendig.

6.1.3. Auslieferung der öffentlichen Schlüssel an Zertifikatsaussteller

Der Certificate Signing Request (CSR) des Zertifikatnehmers wird an die Zertifizierungsstellen (Issuing CAs) zum Zwecke der Zertifizierung im PKCS#10 Format übermittelt. Der gesamte Prozess findet teilautomatisiert statt.

Der Certificate Signing Request der Issuing CAs erfolgt auch im PKCS#10 Format. Allerdings findet dieser Prozess, aufgrund der Offline-Betriebsart der Sachsen Root CA 02, rein manuell statt.

6.1.4. Auslieferung der öffentlichen CA Schlüssel an vertrauende Parteien

Die Auslieferung der öffentlichen CA Schlüssel erfolgt manuell. Des Weiteren werden die öffentlichen Schlüssel der Sachsen PKI Zertifizierungsstellen auf den dafür vorgesehenen Web-URLs bereitgestellt (2.2 Publikation von Zertifizierungsinformationen).

6.1.5. Schlüssellängen

Sachsen PKI CA Schlüssellänge:

- Sachsen Root CA 02 – 4096bit (HSM) – RSA Algorithmus
- ZD CA 02 – 4096bit (HSM) – RSA Algorithmus

Sachsen PKI Maschinen (Authentifikation) Schlüssellänge:

- Sachsen PKI Maschinen Authentifikation (2K) – 2048bit (Software CSP) – RSA Algorithmus

6.1.6. Erzeugung und Prüfung der Schlüsselparameter

Für den RSA Algorithmus nicht zutreffend.

6.1.7. Schlüsselverwendungszweck (wie im X.509 Version 3 Key Usage Feld)

Siehe auch in Abschnitt 7.1 Zertifikats- und CRL Profile

Sachsen PKI CA Schlüsselverwendung:

- Sachen Root CA 02 – Certificate Signing, CRL Signing, Certificate Trust List Signing, Certificate Trust List Signing (offline)
- ZD CA 02 – Certificate Signing, CRL Signing, Certificate Trust List Signing, Certificate Trust List Signing (offline)

Sachsen PKI Maschinen (Authentifikation) Schlüsselverwendung:

- Sachsen PKI Maschinen Authentifzierung (Web Server/Domain Controller) – Digital Signature, Key Encipherment
- Sachsen PKI Maschinen Authentifzierung (Computer Authentication) – Digital Signature

6.2. Schutz des privaten Schlüssels und kryptographische Module

In der Sachsen PKI wird privates Schlüsselmaterial durch kryptographische Module in der Ausprägung als Hardware oder Software geschützt. Der Schutz des privaten Schlüsselmaterials von:

- Sachsen PKI Zertifizierungsstellen wird durch das Hardware Security Modul realisiert.
- Sachsen PKI Maschinen wird durch eine Software Implementierung der Krypto-Schnittstelle realisiert.

6.2.1. Standards und Sicherheitsmaßnahmen von kryptographischen Modulen

- Das eingesetzte HSM ist nach FIPS 140-2, Level 2 und Level 3 evaluiert.
- Die eingesetzten HSM Smartcards sind nach FIPS 140-2, Level 3 evaluiert.
- Die eingesetzten Software Krypto-Module sind nach FIPS 140-2, Level 1 evaluiert.

6.2.2. Mehr-Personenkontrolle von privaten Schlüsseln (n von m Verfahren)

Eine Schlüsselteilung von privaten Schlüsseln findet nicht statt. Ausnahme bildet der Betrieb der HSM. Ein n-von-m Verfahren für die HSM Verwaltung und den Zugriff auf Schlüsselmaterial der Sachsen PKI CAs wurde eingerichtet.

6.2.3. Hinterlegung von privaten Schlüsseln

Nicht zutreffend. Private Schlüssel werden nicht hinterlegt. Zur Wiederherstellung von privatem Schlüsselmaterial steht ein Schlüssel Backup zur Verfügung.

6.2.4. Backup von privaten Schlüsseln

Privates Schlüsselmaterial der Sachsen PKI Zertifizierungsstellen wird durch das etablierte Backup Verfahren in Verbindung mit der HSM Absicherung gesichert.

6.2.5. Archivierung von privaten Schlüsseln

Nicht zutreffend. Private Schlüssel werden aktuell nicht archiviert.

6.2.6. Transfer von privaten Schlüsseln in oder aus einem kryptographischen Modul

Ein Transfer von privaten CA-Schlüsseln ist nicht vorgesehen.

Eine Ausnahme bildet das Verfahren für die authentisierte Antragsstellung von Zertifikaten über die RA-Stelle (CAM-Zertifikatsportal) mit Schlüsselgenerierung durch HSM. Der Schlüssel wird dabei nicht im HSM gespeichert und über die RA-Stelle dem Antragsteller ausgeliefert.

6.2.7. Ablage von privaten Schlüsseln im kryptographischen Modul

Die privaten Schlüssel der Sachsen Root CA 02 und der Issuing CAs werden über das HSM der Zertifizierungsdienste gesichert gespeichert.

6.2.8. Aktivierung der privaten Schlüssel

Nicht zutreffend. Eine Aktivierung von privaten Schlüsseln ist für die Sachsen PKI nicht vorgesehen.

6.2.9. Deaktivierung der privaten Schlüssel

Nicht zutreffend. Eine Deaktivierung von privaten Schlüsseln ist für die Sachsen PKI nicht vorgesehen.

6.2.10. Vernichtung der privaten Schlüssel

Die Methoden zur Vernichtung privater Schlüssel durch den Zertifizierungsdienstanbieter hängen von der kryptographischen Hardware und/oder der kryptographischen Software ab, in der die Schlüssel gespeichert werden:

- Die Vernichtung des gesamten privaten Schlüsselmaterials erfolgt in der Regel durch das Löschen des privaten Schlüsselspeichers. Eine individuelle Löschung von privaten Schlüsseln muss manuell umgesetzt werden.
- Private CA Schlüssel, die über HSMs abgesichert werden, werden durch das Löschen des Schlüssels in Verbindung mit den etablierten HSM Betriebsprozessen vernichtet.
- Private Schlüssel, die auf Smartcards vorliegen, werden durch eine Initialisierung bzw. Formatierung gelöscht. In hochsensiblen Bereichen werden die Smartcards physisch vernichtet.

6.2.11. Bewertung des kryptographischen Moduls

- Das eingesetzte HSM wird nach FIPS 140-2, Level 2 betrieben.
- Die eingesetzten Software Krypto-Module werden nach FIPS 140-2, Level 1 betrieben.

6.3. Weitere Aspekte für die Verwaltung von Schlüsselpaaren

6.3.1. Archivierung der öffentlichen Schlüssel

Alle von den Zertifizierungsdiensten ausgestellten Zertifikate werden in der Zertifizierungsstellendatenbank archiviert. Darüber hinaus findet keine Archivierung öffentlicher Schlüssel statt.

6.3.2. Gültigkeit von Zertifikaten und Schlüsselpaaren.

Für die Sachsen PKI Zertifizierungsstellen und End-Entitäten sind folgende Lebensdauern festgelegt:

- CA Zertifikate:
  - (siehe Abschnitt 1.3.1. Zertifizierungsstellen)
- End-Entitäten::
  - Gültigkeit bis 3 Jahre (bei 4096bit Schlüssel)
  - Gültigkeit bis 1 Jahr (bei 2048bit Schlüssel)

6.4. Aktivierungsdaten

Nicht zutreffend.

6.5. Sicherheitsmaßnahmen für Computer

6.5.1. Spezifische technische Anforderungen von Sicherheitsmaßnahmen für Computer

Für Rechner, die zentrale Funktionen der Zertifizierungsdienste implementieren, sowie alle Rechner, die dem Schutz der Einrichtungen der Zertifizierungsdienste dienen, gelten die folgenden Sicherheitsanforderungen:

- Auf dem Rechner ist nur die für die jeweilige Funktion notwendige Software installiert.
- Der Rechner besitzt nur die für die jeweilige Funktion notwendigen Kommunikationsschnittstellen. Insbesondere sind die Rechner nur in die für ihre Funktion notwendigen Teilnetzwerke integriert.
- Unnötige Funktionen des Betriebssystems und der installierten Software werden – sofern möglich – deaktiviert.
- Falls Sicherheitsrisiken in der verwendeten Software bekannt werden, ergreifen die Systemadministratoren zeitnah die vom Hersteller bzw. von unabhängigen Experten empfohlenen Gegenmaßnahmen. Insbesondere werden beim Betriebssystem und der Software stets die aktuellen Patches gegen bekannte Sicherheitslücken eingespielt (Ausnahme: RootCA)

- Der Zugriff auf die Rechner ist auf das für den Betrieb der Zertifizierungsdienste notwendige Maß beschränkt. Insbesondere werden die Rechner nur durch die verantwortlichen Systemadministratoren verwaltet.
- Nicht mehr benötigte vertrauliche Daten (z.B. Schlüsselmaterial) werden von den Rechnern gelöscht. Die Löschung erfolgt in einer Weise, die eine teilweise oder vollständige Rekonstruktion unmöglich macht.
- Sicherheitskritische Ereignisse auf den Rechnern werden protokolliert.
- Systeme mit hohen Verfügbarkeitsanforderungen sind redundant ausgelegt, so dass bei Ausfall eines Rechners die Funktion erhalten bleibt.
- Mittels unterbrechungsfreier Stromversorgungen und mittels Aggregaten werden Schwankungen in der Stromversorgung ausgeglichen und Stromausfälle bis zu einer Dauer von mehreren Stunden überbrückt.
- Auf den Systemen dürfen nur nach Viren geprüfte Datenträger verwendet werden.
- Die Sicherheit der Systeme wird von den verantwortlichen Administratoren regelmäßig mittels geeigneter Werkzeuge geprüft. Bei Aufdeckung von Sicherheitslücken werden sofort entsprechende Gegenmaßnahmen eingeleitet.

6.5.2. Bewertung der Computersicherheit

Die eingesetzte HSMs sind nach FIPS 140-2, Level 2 und Level 3 validiert und werden nach Level 2 betrieben.

6.6. Technische Kontrollen für den gesamten Lebenszyklus

6.6.1. Sicherheitsmaßnahmen bei der Systementwicklung

Nicht zutreffend.

6.6.2. Sicherheitsmanagement

Nicht zutreffend.

6.6.3. Sicherheitsmaßnahmen für den gesamten Lebenszyklus

In Rahmen des Sicherheitskonzeptes für die Sachsen PKI und die zugehörigen Zertifizierungsstellen werden die notwendigen Sicherheitsmaßnahmen beleuchtet.

6.7. Sicherheitsmaßnahmen im Netz

Die Zertifizierungsdienste implementieren die folgenden Maßnahmen zur Netzwerksicherheit:

- Die internen Netzwerke der Zertifizierungsdienste sind soweit möglich nach dem Schutzbedarf der Systeme aufgeteilt. Die Trennung in Teilnetze erfolgt durch Firewalls.

- Firewalls beschränken den Datenverkehr auf das für den Betrieb notwendige Maß.
- Die Sicherheit der Netzwerke der Zertifizierungsdienste wird mittels geeigneter Werkzeuge (z.B. Penetrationstools) geprüft. Bei Aufdeckung von Sicherheitslücken werden sofort entsprechende Gegenmaßnahmen eingeleitet.

6.8. Zeitstempel

Die Sachsen PKI Zertifizierungsstellen nutzen Zeitstempel bei der Ausgabe von Zertifikaten und Zertifikatssperrlisten. Die verwendete Zeitquelle ist hierbei die lokale Systemuhr des verwendeten Computersystems. Die lokale Systemuhr der Online Server wird regelmäßig mit einer externen Zeitquelle automatisch synchronisiert. Die Zeitsynchronisation der Sachsen Root CA 02 erfolgt manuell bei jedem Start des Offline Systems. Der Einsatz einer vertrauenswürdigen und evaluierten Zeitstempelkomponente ist für die Sachsen PKI Lösung nicht vorgesehen.

7. Zertifikats- und CRL Profil

In Rahmen der X.509 PKI sind Zertifikats- und CRL Profile für die Sachsen PKI definiert. Diese Profile folgen den PKIX Vorgaben nach RFC 5280 und haben insbesondere die Interoperabilitätsaspekte im Fokus. Erweiterungen für die Zertifikats- und CRL Profile sind vorgesehen, soweit diese zum Zwecke der Unterscheidung von Zertifikatstypen genutzt werden können.

7.1. Zertifikatsprofil

Sachsen PKI Zertifikate entsprechen:

- ITU-T Empfehlung X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, Juni 1997.

Sachsen PKI Zertifikatsprofile sind konform:

- RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Januar 1999
- RFC 3280 (löst RFC 2459 ab): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002
- **RFC 5280** (löst RFC 3280 ab): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

7.1.1. Version Number(s)

Die Sachsen Root CA 02 und die Issuing CAs stellen X.509 Version 3 Zertifikate aus.

7.1.2. Certificate Extensions

Folgende Zertifikatserweiterungen werden in den von der Sachsen PKI bereitgestellten Zertifikaten berücksichtigt:

Erweiterung	Wert	Kritisch
Key Usage	(Digital Signature), Certificate Signing, Certificate Trust List Signing, Certificate Trust List Signing (offline)	Ja
Subject Key Identifier	Unique number corresponding to the subject's public key. The key identifier method is used.	Nein
Authority Key Identifier	Unique number corresponding to the authority's public key. The key identifier method is used.	Nein
CRL Distribution Point	Contains the information where the current CRL can be obtained	Nein
Authority Information Access	Contains a link where additional information to the issuing CA can be obtained (ca issuers method)	Nein

Folgende private Zertifikatserweiterungen kommen zur Anwendung:

Erweiterung	OID	Kritisch
Certificate Issuance Policies	1.3.6.1.4.1.7848.1.10.1 (Sachsen PKI CP/CPS OID Referenz)	Nein

7.1.3. Algorithm Object Identifiers

Die Sachsen Root CA 02 erstellt Signaturen mit sha256WithRSA Encryption (OID: 1.2.840.113549.1.1.11) gemäß RFC 5280.

7.1.4. Name Forms

Die von der Sachsen Root CA 02 ausgestellten CA Zertifikate enthalten den Teil- DN (Distinguished Name) im Subject Name und im Issuer Name Feld. Der Aufbau des Subjects erfolgt gemäß RFC 5280 und enthält die Komponenten in folgender Reihenfolge:

- DN = [Subject Name / Issuer Name]
- CN = [Common Name],
- OU = [Organizational Unit],
- DC = [Domain Component],
- DC = [Domain Component],

- DC = [Domain Component].

7.1.5. Name Constraints

nicht zutreffend. Es existieren keine Beschränkungen bezogen auf Namen.

7.1.6. Certificate Policy Object Identifier

Die Sachsen PKI Certificate Policy OID lautet: 1.3.6.1.4.1.7848.1.10.1

7.1.7. Policy Constraints Extension

nicht zutreffend.

7.1.8. Policy Qualifiers Syntax und Semantik

Die Sachsen PKI Certificate Policy Qualifier ID ist: CPS.

Die Sachsen PKI CPS Location wird durch eine URL bereitgestellt:

- *http://secure.sachsen.de/pki/cps/*

7.2. CRL Profil

CRLs werden in Rahmen der Sachsen PKI ausgegeben. Eine Ausgabe von deltaCRLs ist im Falle der Sachsen PKI Zertifizierungsstellen nicht geplant.

Die Basis CRL Felder sind wie folgt festgelegt:

Feld	Wert
Version	Siehe auch 7.2.1. Version Number
Issuer	Contains the Distinguished Name of the issuing CA
This update	Time and date of CRL issuance.
Next update	Time and date of next CRL update.
Signature Algorithm	Designation of algorithm used to sign the certificate. Siehe auch 7.1.3. Algorithm Object Identifiers
Signature	CAs signature

Weitere Zertifikatsvorlagen werden separat verwaltet.

7.2.1. Version Number(s)

Die Sachsen PKI Zertifizierungsstellen stellen CRLs auf Basis X.509 Version 2 aus.

7.2.2. CRL und CRL Entry Extensions

CRL Extensions (Erweiterungen) können aus dem aktuell für die Sachsen Root CA 02 geltenden CRL Profil entnommen werden. Siehe auch 7.2. CRL Profile.

7.3. OCSP Profil

OCSP wird im Rahmen der Sachsen PKI genutzt.

7.3.1. Version Number(s)

nicht zutreffend.

7.3.2. OCSP Extensions

nicht zutreffend.

8. Auditierung und Überprüfung der Konformität

In Rahmen der Sachen PKI werden interne Audits durchgeführt, um Abweichungen vom Regelbetrieb der Sachsen PKI zu den Ausführungen in der Sachsen Certificate Policy bzw. Certification Practice Statement (CP/CPS) zu identifizieren und bei aufgedeckten Abweichungen der Konformität notwendige korrektive Maßnahmen zu ergreifen.

8.1. Frequenz und Umstand der Überprüfung

Grundsätzlich sind interne Audits und Überprüfungen in regelmäßigen Abständen geplant. Frequenz und Umstände, die zu einer Überprüfung führen können, werden durch die PKI-Aufsicht / Projektleitung Sachsen PKI festgelegt.

8.2. Identität und Qualifikation des Prüfers/Auditors

Es wird vorgesehen, dass nur interne Mitarbeiter die Konformitätsüberprüfung durchführen. Das Auditierungspersonal sollte über Know-How aus der Auditierung im Sicherheitsumfeld verfügen, insbesondere die notwendigen Kenntnisse aus dem Bereich der Public Key Infrastructure (PKI) und aus dem Bereich des Rechenzentrumsbetriebes sind zwingend erforderlich.

8.3. Verhältnis des Prüfers zur überprüften Entität

Der zugewiesene Auditor für die Überprüfung der Konformität ist zur überprüften Entität, nämlich der Sachsen PKI (Technologie und Prozesse) organisatorisch unabhängig.

8.4. Von der Überprüfung abgedeckte Bereiche

Die von einer Überprüfung betroffenen Bereiche werden jeweils durch die zuständige Zertifizierungsstelle festgelegt. Für Umstände, die zwingend eine Überprüfung notwendig machen, können bestimmte Bereiche von vornherein festgelegt werden.

Dazu gehören unter anderem:

- Key Management Operations
- Certificate Lifecycle Processes
- Data Processing Security and Operations

8.5. Maßnahmen bei Nichterfüllung oder Abweichen von der Konformität

Werden Abweichungen zur Konformität festgestellt so müssen diese zeitnah korrigiert werden. Hierzu wird ein Aktionsplan entwickelt, welcher die notwendigen Maßnahmen beschreibt, um die notwendigen Korrekturen auszuführen. Die Entwicklung und Implementierung des Aktionsplans obliegt der zuständigen Organisationseinheit.

Nach Umsetzung des Aktionsplans gilt es zu überprüfen, ob die ausgeführten Maßnahmen zu einer Korrektur der Mängel geführt haben. Das für die Sachsen PKI zuständige leitende Gremium im Freistaat Sachen wird über die erzielten Ergebnisse informiert.

8.6. Kommunikation der Prüfergebnisse

Die Ergebnisse der Auditierung bzw. Prüfung werden als vertraulich erachtet und sind nicht für die Öffentlichkeit bestimmt. Die zuständige Organisationseinheit kann in besonderen Fällen eine Veröffentlichung der Prüfergebnisse veranlassen.

9. Weitere rechtliche und geschäftliche Regelungen

Dieser Abschnitt bezieht sich auf die geschäftlichen, rechtlichen und Datenschutz-Aspekte der Sachsen PKI.

9.1. Gebühren

Keine.

9.1.1. Gebühren für die Ausstellung und Erneuerung von Zertifikaten

Keine.

9.1.2. Gebühren für den Zugriff auf Zertifikate

Keine.

9.1.3. Gebühren für den Zugriff auf Sperrlisten- oder Status-Information

Keine.

9.1.4. Gebühren für weitere Dienste

Keine.

9.1.5. Richtlinie für die Erstattung von Gebühren

Keine.

9.2. Finanzielle Verantwortung

9.2.1. Versicherungsschutz

Ein gesonderter Versicherungsschutz für die Sachsen PKI ist nicht gegeben.

9.2.2. Vermögenswerte

Vermögenswerte werden nicht abgedeckt.

9.2.3. Versicherungsschutz oder Gewährleistung für Zertifikatsnehmer

Ein Versicherungsschutz für Zertifikatnehmer ist nicht gegeben.

9.3. Vertraulichkeit von Geschäftsinformationen

9.3.1. Vertrauliche Informationen berücksichtigt

Jegliche Informationen über Teilnehmer und Antragsteller, die nicht unter 9.3.2. Vertrauliche Informationen nicht berücksichtigt fallen, werden als vertrauliche Informationen eingestuft. Zu diesen Informationen zählen u. a. Geschäftspläne, Vertriebsinformationen, Informationen über Geschäftspartner und ebenso alle Informationen, die beim Registrierungsprozess zur Kenntnis gekommen sind.

9.3.2. Vertrauliche Informationen nicht berücksichtigt

Jegliche Informationen, die in den herausgegebenen Zertifikaten und Widerrufslisten explizit (z.B. E-Mail Adresse) oder implizit (z.B. Daten über die Zertifizierung) enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft.

9.3.3. Verantwortung zum Schutz vertraulicher Informationen

Jede innerhalb der Sachsen PKI operierende Zertifizierungsstelle trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen.

9.4. Datenschutz (personenbezogen)

9.4.1. Datenschutzrichtlinie/-plan

Die Speicherung und Verarbeitung von personenbezogenen Daten richtet sich nach den gesetzlichen Datenschutzbestimmungen.

9.4.2. Vertraulich zu behandelnde Informationen

Jegliche Informationen über Zertifikatsnehmer und Antragsteller sind vertraulich zu behandeln.

9.4.3. Nicht vertraulich zu behandelnde Informationen

Nicht vertraulich sind Informationen, die in den öffentlichen Zertifikaten, wie in den Sachsen PKI Zertifizierungsstellenzertifikaten, enthalten sind. Ebenfalls gilt es für Informationen, die in den öffentlichen Zertifikatssperrlisten (CRLs) enthalten sind.

9.4.4. Verantwortung zum Schutz personenbezogener Information

Der Sachsen PKI Betrieb ist verantwortlich für den Schutz vertraulicher Informationen. Eine Offenlegung von vertraulichen Informationen kann nur in Abstimmung mit den verantwortlichen Stellen geschehen.

9.4.5. Benachrichtigung bei Nutzung personenbezogener Information

Der Zertifikatnehmer stimmt der Nutzung von personenbezogenen Daten durch eine Zertifizierungsstelle zu, soweit dies zur Leistungserbringung erforderlich ist. Darüber hinaus können alle Informationen veröffentlicht werden, die als nicht vertraulich behandelt werden.

9.4.6. Offenlegung bei gerichtlicher Anordnung oder in Rahmen einer gerichtlichen Beweisführung

Die Sachsen PKI richtet sich bei der Speicherung und Verarbeitung von personenbezogenen Daten nach den gesetzlichen Datenschutzbestimmungen. Eine Offenlegung findet nur gegenüber staatlichen Instanzen statt, wenn entsprechende richterliche Anordnungen ausgegeben wurden.

9.4.7. Andere Umstände einer Veröffentlichung

Keine.

9.5. Urheberrechte

Der Freistaat Sachen besitzt die Urheberrechte für ausgegebene Dokumentationen in Rahmen der Sachsen PKI.

9.6. Verpflichtungen

9.6.1. Verpflichtung der Zertifizierungsstellen

Die Sachsen PKI Zertifizierungsstellen und sämtliche teilnehmenden Instanzen und Nutzer verpflichten sich den aufgestellten Bestimmungen der CP bzw. CPS Dokumentation zu folgen.

9.6.2. Verpflichtung der Registrierungsstellen

Die Sachsen PKI Registrierungsstellen verpflichten sich den aufgestellten Bestimmungen der CP bzw. CPS Dokumentation zu folgen.

9.6.3. Verpflichtung des Zertifikatsnehmers

Die Nutzung der Zertifikate durch den Zertifikatsnehmer hat den Sachsen PKI Zertifikatsrichtlinien zu folgen. Im Abschnitt 1.4. Anwendungsbereich von Zertifikaten sind die zulässigen und unzulässigen Anwendungen der Schlüssel bzw. Zertifikate festgelegt. Außerdem muss der Zertifikatsnehmer bei der Nutzung der privaten Schlüssel seine in der Zertifikatsrichtlinie definierten Pflichten erfüllen.

9.6.4. Verpflichtung der vertrauenden Partei

Die Nutzung der Zertifikate durch vertrauende Parteien hat den zugewiesenen Zertifikatsrichtlinien seiner Organisation zu folgen. Dort sind die zulässigen und unzulässigen Anwendungen der Schlüssel bzw. Zertifikate festgelegt.

9.6.5. Verpflichtung anderer Teilnehmer

Nicht zutreffend, da keine anderen Teilnehmer vorgesehen sind.

9.7. Gewährleistung

Grundsätzlich wird keine Gewährleistung übernommen. Der Freistaat Sachsen bzw. der im Auftrag handelnde Dienstleistungspartner stellt die notwendigen IT Ressourcen für den Betrieb der PKI entsprechend der für die zentralen Dienste des SVN vereinbarten Verfügbarkeiten zur Verfügung.

9.8. Haftungsbeschränkung

Der Freistaat Sachsen bzw. der im Auftrag handelnde Dienstleistungspartner übernehmen keinerlei Haftung für Sach- und Vermögensschäden. Insbesondere bei einer unsachgemäßen oder einer grob fahrlässigen Nutzung der Sachsen PKI erlischt jegliche Haftung gegenüber Dritten.

9.9. Haftungsfreistellung

Bei der unsachgemäßen Verwendung des Zertifikats und des zu Grunde liegenden privaten Schlüssels oder einer Verwendung des Schlüsselmaterials beruhend auf fälschlichen oder fehlerhaften Angaben bei der Beantragung, ist der Freistaat Sachsen bzw. der im Auftrag handelnde Dienstleistungspartner von der Haftung freigestellt.

9.10. Inkrafttreten und Aufhebung

9.10.1. Inkrafttreten

Die CP/CPS Dokumentation tritt mit Veröffentlichung in Kraft. Die Veröffentlichung erfolgt auf der im Zertifikat vorgegebenen URL:

- *http://secure.sachsen.de/pki/cps/*

9.10.2. Aufhebung

Dieses Dokument ist solange gültig, bis

- es durch eine neue Version ersetzt wird oder
- der Betrieb der Sachsen PKI Zertifizierungsstellen eingestellt wird.

9.10.3. Konsequenzen der Aufhebung

Keine.

9.11. Individuelle Benachrichtigung und Kommunikation mit Teilenehmern

Die individuelle Benachrichtigung der Sachsen PKI Teilnehmer obliegt der betriebsführenden Organisationseinheit.

9.12. Ergänzungen der Richtlinie

Die Ergänzung und Modifikation der CP bzw. CPS Dokumentation obliegt der PKI-Aufsicht / Projektleitung Sachsen PKI. In Abschnitt 1.5. Verwaltung der Richtlinien sind entsprechende Kontaktdaten veröffentlicht.

9.12.1. Prozess für die Ergänzung der Richtlinie

Nicht zutreffend.

9.12.2. Benachrichtigungsmethode und -zeitraum

Nicht zutreffend.

9.12.3. Bedingungen für die Änderung einer OID

Nicht zutreffend.

9.13. Schiedsverfahren

Nicht zutreffend.

9.14. Gerichtsstand

Gerichtsstand: Dresden

Der Betrieb der Sachsen PKI unterliegt den Gesetzen der Bundesrepublik Deutschland. Der Gerichtsstand ist Dresden, Bundesrepublik Deutschland. Dieser Gerichtsstand gilt auch für Parteien, deren Wohnsitz oder der gewöhnlicher Aufenthaltsort ins Ausland verlegt wird oder unbekannt ist.

9.15. Konformität zum geltenden Recht

Die von der Sachsen PKI ausgestellten Zertifikate sind nicht konform zu qualifizierten Zertifikaten. Die Vorgaben und Richtlinien nach deutschem Signaturgesetz [SigG] sind daher nicht bindend für den Betrieb der Sachsen PKI.

9.16. Weitere Regelungen

9.16.1. Vollständigkeit

Alle in der CP/CPS für die Sachsen PKI beschriebenen Regelungen gelten für die vom Freistaat Sachsen bzw. dem im Auftrag handelnden Dienstleistungspartner betriebenen Zertifizierungsstellen und deren Zertifikatnehmern. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2. Übertragung der Rechte

Eine Übertragung der Rechte ist nicht vorgesehen.

9.16.3. Salvatorische Klausel

Sollten einzelne Bestimmungen dieses CP/CPS Regelwerkes unwirksam sein oder dieses Regelwerk Lücken enthalten, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt.

Anstelle der unwirksamen Bestimmungen gilt diejenige wirksame Bestimmung, welche dem Sinn und Zweck der unwirksamen Bestimmung entspricht. Im Falle von Lücken, gilt dasjenige, was nach Sinn und Zweck dieses Dokumentes vernünftigerweise vereinbart worden wäre, hätte man die Angelegenheit von vornherein bedacht.

Es wird ausdrücklich vereinbart, dass sämtliche Bestimmungen dieser CP/CPS, die eine Haftungsbeschränkung, den Ausschluss oder die Beschränkung von Gewährleistungen oder sonstigen Verpflichtungen oder den Ausschluss von Schadensersatz vorsehen, als eigenständige Regelungen und unabhängig von anderen Bestimmungen bestehen und als solche durchzusetzen sind.

9.16.4. Erzwingungsklausel

Rechtliche Auseinandersetzungen, die aus dem Betrieb einer vom Freistaat Sachsen bzw. dem im Auftrag handelnden Dienstleistungspartner betriebenen Zertifizierungsstelle herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland.

Erfüllungsort und ausschließlicher Gerichtsstand ist Dresden, Bundesrepublik Deutschland.

9.16.5. Höhere Gewalt

Der Freistaat Sachsen bzw. der im Auftrag handelnde Dienstleistungspartner übernimmt keine Haftung für die Verletzung einer Pflicht sowie für Verzug oder Nichterfüllung im Rahmen dieses CPS, sofern dies aus Ereignissen außerhalb ihrer Kontrolle, wie z.B. höhere Gewalt, Kriegshandlungen, Epidemien, Netzausfälle, Brände, Erdbeben und andere Katastrophen, resultiert.

9.17. Andere Regelung

Keine.

Herausgeber & Redaktion
Sächsisches Staatsministerium des Innern
Wilhelm-Buck-Straße 4
01097 Dresden

Verteilerhinweis

Diese Informationsschrift wird von der Sächsischen Staatsregierung im Rahmen ihrer verfassungsmäßigen Verpflichtung zur Information der Öffentlichkeit herausgegeben. Sie darf weder von Parteien noch von deren Kandidaten oder Helfern im Zeitraum von sechs Monaten vor einer Wahl zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für alle Wahlen.

Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist auch die Weitergabe an Dritte zur Verwendung bei der Wahlwerbung. Auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl darf die vorliegende Druckschrift nicht so verwendet werden, dass dies als Parteinahme des Herausgebers zu Gunsten einzelner politischer Gruppen verstanden werden könnte.

Diese Beschränkungen gelten unabhängig vom Vertriebsweg, also unabhängig davon, auf welchem Wege und in welcher Anzahl diese Informationsschrift dem Empfänger zugegangen ist. Erlaubt ist jedoch den Parteien, diese Informationsschrift zur Unterrichtung ihrer Mitglieder zu verwenden.