CP/CPS
Landschaftsverband Rheinland PKI G2

Zertifikatsrichtlinie (CP) &
Erklärung zum Zertifizierungsbetrieb (CPS)

Version: 1.0.3

Stand: 06.02.2017

Status: Abgenommen

Autor/in: Andreas Lucas (Microsoft GmbH),
Andreas Neppach (Microsoft GmbH)
Gürkan Aydin (LVR-InfoKom)

Besitzer/in: Gürkan Aydin

Vertraulichkeitsklassifizierung: öffentlich

LVR-InfoKom, Ottoplatz 2, D-50679 Köln

Tel.: 0221 809 7650
Internet: www.infokom.lvr.de

Obwohl das Dokument mit großer Sorgfalt erstellt und geprüft wurde, können Fehler nicht vollkommen ausgeschlossen werden. Fehlerhinweise werden gerne unter Angabe des Dokumentes seitens der Autoren/innen unter o. a. Anschrift entgegengenommen.

Versionshistorie

Version	Datum	Name	Änderung
1.0.0	27.07.2016	Andreas Lucas	Konsolidierte Version für Root und Sub CA
1.0.1	17.10.2016	Gürkan Aydin	Korrekturen und Anpassungen von diversen Kapiteln
1.0.2	24.11.2016	Andreas Neppach	Korrekturen und Anpassungen von diversen Kapiteln
1.0.3	23.01.2017	Gürkan Aydin	Korrekturen und Anpassungen von diversen Kapiteln

Abnahmehistorie

Version	Datum	Beschlossen durch	Hinweise
1.0.3	06.02.2017	Philipp Franzen	

Inhaltsverzeichnis

1 Einleitung

Der Begriff „Certificate Policy (CP)", definiert im X.509 Standard, steht für die Gesamtheit der Regeln und Vorgaben, welche die 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 und Anwendung vertraut werden kann.
Insbesondere sollte eine CP darlegen:

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

Das Konzept einer "Certification Practice Statement (CPS)" wurde von der American Bar Association (ABA) entwickelt und ist in deren Digital Signature Guidelines (ABA Guidelines) aufgeführt. Die CPS ist eine detaillierte Beschreibung des Zertifizierungsbetriebes der Organisation. Aus diesem Grund stellen Organisationen, die eine oder mehrere Zertifizierungsstellen betreiben, in der Regel auch eine CPS zur Verfügung. In Rahmen einer unternehmensweiten PKI ist die CPS für Organisationen ein adäquates Mittel um sich selbst zu schützen, sowie Geschäftsvorfälle zu Zertifikatsnehmern und vertrauenden Parteien darzustellen.
Ein zentraler Aspekt der CP/CPS Vorlage für den Landschaftsverband Rheinland (LVR) ist die Bestimmung der Vertrauenswürdigkeit auszugebender Zertifikate und des Zertifizierungsdienstes betrieben durch das Rechenzentrum des LVR. Mit Teilnahme an den LVR-Zertifizierungsdiensten akzeptieren die LVR-Mitarbeiter und vertrauende Parteien, z.B. im IT-Verbund angeschlossenen Kliniken, die Bedingungen und Regularien aufgeführt im CP/CPS.
Die Dokumentenstruktur orientiert sich an dem im RFC 3647 angegebenen Empfehlungen. Entsprechend den Vorgaben des RFC 3647 legt die LVR CP/CPS die Vorgehensweise dar, die der Zertifizierungsdienst bei der Beantragung, Generierung, Auslieferung und Verwaltung der Zertifikate anwendet.
Aufgrund der Anforderung einer vereinfachten Dokumentenverwaltung wurden die CP (Certificate Policies) und CPS (Certification Practice Statement) in einem zentralen Dokument zusammenzufassen. Dieses Dokument beschreibt die **Zertifikatsrichtlinie und die Erklärung zum Zertifizierungsbetrieb der LVR PKI G2 des Landschaftsverbandes Rheinland**. Die Verteilung dieses Dokuments ist kostenfrei und öffentlich zugänglich für LVR-Mitarbeiter.

1.1 Überblick

LVR-InfoKom betreibt Zertifizierungsdienste für die Erzeugung, Ausgabe und Verwaltung von Zertifikaten. Die LVR G2 Root CA 01 erlaubt die automatisierte und kontrollierte Ausgabe von Zertifikaten bzw. Smartcards. Das untenstehende Schaubild gibt einen Überblick über die LVR PKI G2. Die LVR-Zertifizierungsinfrastruktur ist hierarchisch aufgebaut und terminiert an der LVR G2 Root CA 01.
Neben den installierten CAs wird ein Zertifikatsmanagementsystem sowie Enrollment Service betrieben.
Für das Enrollment von Maschinenzertifikaten, stehen neben dem klassischen auf DCOM basierende Enrollment auch NDES- und CEP/CES-Enrollment Services zur Verfügung. Weitergehende Informationen zu den Enrollment Services können auf Wunsch angefordert werden. Die Kontaktinformationen sind aus Kapitel 3.2 Kontaktpersonen zu entnehmen.

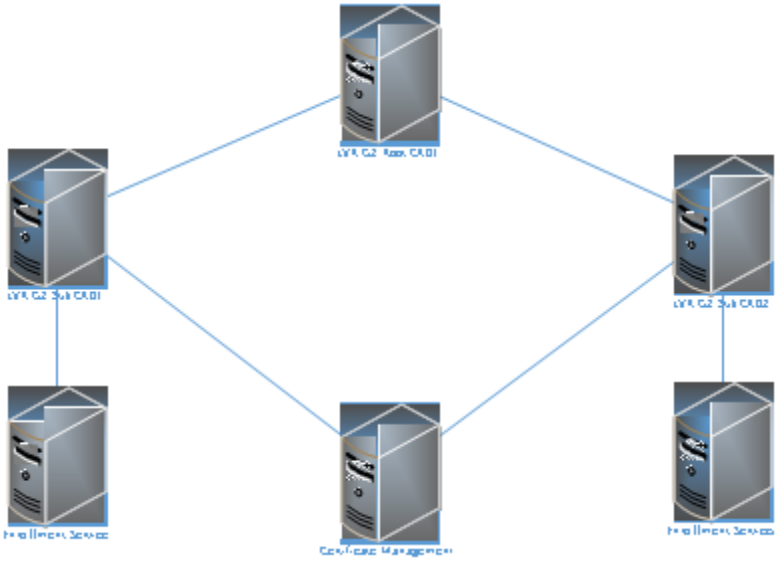

Figure 1: LVR PKI G2-Umgebung

1.2 Beschreibung der Zertifikatsinstanzen

Die Funktionen der einzelnen Zertifizierungsinstanzen sind in den folgenden Kapiteln beschrieben. Weitergehende Informationen zur PKI Architektur können auf Wunsch angefordert werden. Die Kontaktinformationen sind aus Kapitel 3.2. Kontaktpersonen zu entnehmen.

1.2.1 LVR G2 Root CA 01

Die Zertifizierungsinstanz LVR G2 Root CA 01 ist der Vertrauensanker der LVR PKI G2. Die Zertifizierungsinstanz wird ausschließlich zu Signierung von Sub CA verwendet. Das Ausstellen von End-Entitäten ist nicht vorgesehen.

1.2.2 LVR G2 Sub CA 01

Die Zertifizierungsinstanz LVR G2 Sub CA 01 wird zur Ausstellung von Benutzerzertifikaten verwendet. Hierzu gehören Zertifikate der folgenden Kategorien:

- SmartCard Logon-Zertifikate zur sicheren Autorisierung von Benutzern am LVR Active Directory
- S/MIME Zertifikate zur sicheren Identifikation von E-Mail Absendern sowie für eine End-zu-End Verschlüsselung des E-Mail-Verkehrs

- Authentifizierungs-Zertifikate zur sicheren Autorisierung von Benutzern an Webdiensten.

1.2.3 LVR G2 Sub CA02

Die Zertifizierungsinstanz LVR G2 Sub CA 02 wird zur Ausstellung von Maschinenzertifikate verwendet. Hierzu gehören Zertifikate der folgenden Kategorien:

- Computer Zertifikate zur Identifikation von Computer
- Computer Zertifikate zur Identifikation von Netzwerk-Infrastruktur Komponenten
- Computer Zertifikate zur Identifikation von Mobilen-Endgeräten
- VPN Zertifikate für eine gesicherte Kommunikation über unsichere Netzwerke (z.B. Internet)
- IPsec Zertifikate für eine gesicherte und identifizierte Kommunikation über unsichere Netzwerke (z.B. Internet)
- Transport Layer Zertifikate für die verschlüsselte Kommunikation über unsichere Netzwerke oder für besonders schützenswerte Daten.

1.3 Dokumentation und Identifikation

Dies sind die **Zertifikatsrichtlinie und die Erklärung zum Zertifizierungsbetrieb der LVR G2 Root CA des Landschaftsverbandes Rheinland**. Ein eindeutiger ASN.1 Object Identifier (OID) ist diesem Dokument zugewiesen. Die LVR OID ist bei der iana.org registriert, siehe auch:
http://www.iana.org/assignments/enterprise-numbers
Kontaktperson:
Landschaftsverband Rheinland (formerly 'LVR-InfoKom')
Philipp Pfaff
Ottoplatz 2
50679 Köln
Tel.: +49 (221)809-7650
Mail: zv.z13.app@lvr.de
Web: infokom.lvr.de

- **LVR Enterprise OID:** 1.3.6.1.4.1.28973
  OID Beschreibung: Landschaftsverband Rheinland (formerly 'LVR-InfoKom') Private Enterprise Code

- **LVR PKI OID:** 1.3.6.1.4.1.28973.509
  OID Beschreibung: Namensraum der X.509 PKI Dienste des LVR-InfoKom

- **LVR G2 PKI OID:** 1.3.6.1.4.1.28973.509.2
  OID Beschreibung: Namensraum der LVR PKI Generation 2

- **LVR G2 PKI OID:** 1.3.6.1.4.1.28973.509.2.20
  OID Beschreibung: Namensraum der Produktionsumgebung

- **LVR G2 PKI OID:** 1.3.6.1.4.1.28973.509.2.20.10
  OID Beschreibung: PKI Richtlinien und Richtlinien Referenz Nummernkreis

- **LVR G2 PKI OID:** 1.3.6.1.4.1.28973.509.2.20.10.1
  OID Beschreibung: Referenz der LVR G2 PKI Issuance Policy

- **LVR G2 PKI OID:** 1.3.6.1.4.1.28973.509.2.20.20
  OID Beschreibung: PKI Dokumenten Nummernkreis

- **LVR G2 PKI OID:** 1.3.6.1.4.1.28973.509.2.20.20.1
  OID Beschreibung: CP/CPS Dokumentbezeichner

- **LVR G2 PKI OID:** 1.3.6.1.4.1.28973.509.2.20.20.1.X
  OID Beschreibung: CP/CPS Dokumentenversion

- **Der CP/CPS Titel lautet:**
  CP/CPS des Landschaftsverband Rheinland PKI G2 –
  Zertifikatsrichtlinie (CP) & Erklärung zum Zertifizierungsbetrieb (CPS)

- **LVR PKI G2 CP/CPS OID:** 1.3.6.1.4.1.28973.509.2.20.20.1.1
  OID Beschreibung: OID für CP/CPS des Landschaftsverband Rheinland PKI G2 – Zertifikatsrichtlinie (CP) & Erklärung zum Zertifizierungsbetrieb (CPS)

- **LVR PKI G2 Issuance Policy OID:** 1.3.6.1.4.1.28973.509.2.20.10.1
  OID Beschreibung: OID für die Issuance Policy des Landschaftsverband Rheinland PKI G2

Der Object Identifier (OID) für die Dokumentation setzt sich wie folgt zusammen:
{iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) LVR (28973) X509 (509) LVR PKI Generation 2(2) Produktion (20) Dokumenten Nummernkreis (20) CP/CPS Bezeichner (1) Version 1 (1)}

Der Object Identifier (OID) für die Issuance Policy setzt sich wie folgt zusammen:
{iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) LVR (28973) X509 (509) LVR PKI Generation 2(2) Produktion (20) PKI Richtlinien Referenz (10) Issuance Policy Referenz (1)}

Die Lokation der LVR-InfoKom CP/CPS Dokumentationen für LVR Zertifikatsnehmer und vertrauende Parteien lautet: http://www.pki.lvr.de
Der vollständige Distiguished Name (DN) der beteiligten CAs lautet:

- **LVR G2 Root CA 01**
  CN = LVR G2 Root CA 01
  O = Landschaftsverband Rheinland
  C = DE
- **LVR G2 Sub CA 01**
  CN = LVR G2 Sub CA 01
  O = Landschaftsverband Rheinland
  C = DE
- **LVR G2 Sub CA 02**
  CN = LVR G2 Sub CA 02
  O = Landschaftsverband Rheinland
  C = DE

1.4 Weitere unterstützte Zertifikatsrichtlinien

Alle CAs unterstützen alle Applikationsrichtlinien.

1.5 Zertifizierungsstellen

Die LVR PKI G2 basiert auf drei aufgelisteten Zertifizierungsstellen.

Zertifizierungsstelle	Laufzeit	CRL Laufzeit
LVR G2 Root CA 01	15 Jahre	3 Monate + 1 Monat Überlappungszeitraum
LVR G2 Sub CA 01	7 Jahre	7 Tage + 3 Tage Überlappungszeitraum
LVR G2 Sub CA 02	7 Jahre	7 Tage + 3 Tage Überlappungszeitraum

1.5.1 LVR G2 Root CA 01

Die LVR G2 Root CA 01 basiert auf einem selbst-signierten CA-Zertifikat. Die LVR G2 Root CA 01 ist von Produktionsnetz entkoppelt und unterhält eine dedizierte Verbindung zum Hardware Security Module (HSM). Die LVR G2 Root CA 01 befindet sich im Offline Betrieb und wird zu keiner Zeit in irgendeiner Art und Weise mit dem Client-Netzwerk verbunden. Alle kryptographischen Operationen der LVR G2 Root CA 01 werden durch das HSM ausgeführt.
Die LVR Root CA 01 stellt CA-Zertifikate und Sperrlisten für subordinierte Zertifizierungsstelleninstanzen (LVR Sub CAs), wie auch für sich selbst aus.

Für die LVR G2 Root CA 01 wurde folgende Lebensdauern festgelegt:

- LVR G2 Root CA 01 Zertifikat:
  15 Jahre
- Root CA CRLs:
  3 Monate (3 Monate Publikationsintervall und 1 Monat Überlappungszeitraum)

1.5.2 LVR G2 Sub CA 01

Die LVR G2 Sub CA 01 basiert auf einem CA-Zertifikat, welches von der LVR G2 Root CA 01 signiert wurde. Bei der LVR G2 Sub CA 01 handelt es sich um eine Online-CA, die mit dem Intranet der LVR verbunden ist. Die LVR G2 Sub CA 01 wird durch eine Netzwerk-Firewall gegen unberechtigte Zugriffe geschützt.
Das private Schlüsselmaterial der LVR G2 Sub CA 01 wird durch ein HSM geschützt.
Die LVR G2 Sub CA 01 stellt CA-Zertifikate und Sperrlisten für End-Identitäten aus.
Für die LVR G2 Sub CA 01 wurde folgende Lebensdauern festgelegt:

- LVR G2 Sub CA 01 Zertifikat:
  7 Jahre
- Publizierte Sperrlisten (CRLs):
  10 Tage(7 Tage Publikationsintervall und 3 Tage Überlappungszeitraum)

1.5.3 LVR G2 Sub CA 02

Die LVR G2 Sub CA 02 basiert auf einem CA-Zertifikat, welches von der LVR G2 Root CA 01 signiert wurde. Bei der LVR G2 Sub CA 02 handelt es sich um eine Online-CA, die mit dem Intranet der LVR verbunden ist. Die LVR G2 Sub CA 02 wird durch eine Netzwerk-Firewall gegen unberechtigte Zugriffe geschützt.
Das private Schlüsselmaterial der LVR G2 Sub CA 02 wird durch ein HSM geschützt.
Die LVR G2 Sub CA 02 stellt End-Identitäten Zertifikate und Sperrlisten aus.
Für die LVR G2 Sub CA 02 wurde folgende Lebensdauern festgelegt:

- LVR G2 Sub CA 02 Zertifikat:
  7 Jahre
- Publizierte Sperrlisten (CRLs):
  10 Tage (7 Tage Publikationsintervall und 3 Tage Überlappungszeitraum)

1.6 Registrierungsstellen

Einer Registrierungsstelle (RA) obliegt die Überprüfung der Identität und Authentizität von Teilnehmern und Zertifikatsinhabern. Diese Aufgabe werden von der LVR-InfoKom übernommen.

1.6.1 Registrierungsstellen LVR G2 Root CA 01

Zur Identifikation natürlicher Personen kann sich die LVR-InfoKom von der LVR angebotenen HR Service bedienen.

1.6.2 Registrierungsstellen LVR G2 Sub CA 01

Die Registrierungsstelleninstanzen im Sinne dieser Certificate Policy sind Instanzen, welche die Zertifikatsnehmer und Antragssteller erfassen und identifizieren und auch für Zertifikatsnehmer Zertifikate beantragen. Die Registrierungsstelle für die LVR G2 Sub CA 01 ist mittels einem Zertifikatsmangementsystem implementiert.
Die zentrale Aufgabenstellung ist die Bereitstellung von externen Teilnehmerzertifikaten für die Kommunikation zu den vertrauenden Parteien. Die Zertifikatsbeantragung für die

Zertifikatsnehmer erfolgt manuell nach den Prozessen der Registrierungsstelle oder automatisiert, sofern die Identitäten durch den LVR Verzeichnisdienst identifiziert und autorisiert worden sind. Registrierungsstellen können auch durch autorisierte Identitäten in Form von Autorisierungszertifikaten (Enrollment-Agent) realisiert werden.

1.6.3 Registrierungsstellen LVR G2 Sub CA 02

Einer Registrierungsstelle (RA) obliegt die Überprüfung der Identität und Authentizität von Teilnehmern und Zertifikatsinhabern. Diese Aufgabe werden von der LVR-InfoKom übernommen.

- Zur Identifikation natürlicher Personen kann sich die LVR-InfoKom von der LVR angebotenen HR Service sowie dem etablierten LVR Verzeichnisdienst bedienen.
- Zur Identifikation von Computer kann sich die LVR-InfoKom dem LVR Verzeichnisdienst bedienen.

1.7 Teilnehmer und Instanzen

Die Teilnehmer der LVR G2 Root CA 01 sind ausschließlich Sub CAs innerhalb der LVR PKI Infrastruktur oder Sub CAs die eine entsprechende Vereinbarung mit dem Landschaftsverband Rheinland getroffen haben.
Die Teilnehmer der LVR G2 Sub CA 01 und der LVR G2 Sub CA 02 sind ausschließlich validierte End-Identitäten innerhalb der LVR PKI Infrastruktur. Die Identitäten können durch den LVR Verzeichnisdienst validiert werden. Eine Validierung von zusätzlichen Identitäten ist erlaubt, wenn diese durch die LVR-InfoKom zuvor validiert worden sind.

1.7.1 Zertifikatsnehmer

- Zertifikatsnehmer der LVR G2 Root CA 01 sind ausschließlich Sub-CA Entitäten des Landschaftsverbands Rheinland.
- Zertifikatsnehmer der LVR G2 Sub CA 01 sind ausschließlich End-Entitäten des Landschaftsverbands Rheinland. Dies sind ausschließlich Teilnehmer im LVR Verzeichnisdienst.
- Zertifikatsnehmer der LVR G2 Sub CA 02 sind ausschließlich End-Entitäten des Landschaftsverbands Rheinland. Dies sind Teilnehmer im LVR Verzeichnisdienst sowie durch die RA validierte Entitäten.

1.7.2 Weitere Teilnehmer

Nichtzutreffend.

2 Anwendungsbereich von Zertifikaten

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

2.1 Zulässige Anwendung von Zertifikaten

2.1.1 Zulässige Anwendung von Zertifikaten für LVR G2 Root CA 01

Die von der LVR G2 Root CA 01 ausgestellten Zertifikate dürfen ausschließlich für Sub-CA im Rahmen der LVR PKI verwendet werden.
Die im Rahmen dieser CP/CPS ausgestellten Zertifikate können durch den Zertifikatsnehmer für delegierte Funktionen einer Sub-CA verwendet werden.

2.1.2 Zulässige Anwendung von Zertifikaten für LVR G2 Sub CA 01

Die von der LVR G2 Sub CA 01 ausgestellten Zertifikate dürfen zum Zwecke

- der Benutzer Autorisierung im LVR Verzeichnisdienst
- der Benutzer Autorisierung in LVR validierten Applikationen
- sicheren Identifizierung von E-Mail Absendern
- geschützten Kommunikation von E-Mails

verwendet werden.

2.1.3 Zulässige Anwendung von Zertifikaten für LVR G2 Sub CA 02

Die von der LVR G2 Sub CA 02 ausgestellten Zertifikate dürfen zum Zwecke

- der Identifikation von Computer
- der Identifikation von Netzwerk-Infrastruktur Komponenten
- der Identifikation von Mobilen-Endgeräten
- Verschlüsselung von Kommunikation in unsicheren Umgebungen (VPN/IPsec)
- Verschlüsselung der Kommunikation von besonders schützenswerten Daten (TLS)

verwendet werden.

2.2 Unzulässige Anwendung von Zertifikaten

Die Zertifikatsnutzung ist innerhalb der LVR PKI G2 beschränkt und nur für den Einsatz der vorgegebenen Anwendungsbereiche zulässig. Eine Anwendung der Zertifikate für den privaten Gebrauch ist ebenso untersagt, wie auch die Nutzung dieser Zertifikate für andere Anwendungszwecke abweichend von Kapitel 2 Zulässige Anwendungen von Zertifikaten.
Jegliche weitere Zertifikatsnutzung ist untersagt, insbesondere die Zertifizierung weiterer, untergeordneter Zertifizierungsstellen ist ausschließlich der LVR PKI G2 vorbehalten.
Die Einhaltung der LVR CP/CPS Konformität ist jegliche Änderung oder Erweiterung der Zertifikatsanwendung unverzüglich der LVR PKI G2 Administration anzuzeigen.

3 Verwaltung der Richtlinien

3.1 Organisation

LVR-InfoKom ist die verantwortliche Organisation für die Verwaltung der Zertifikatsrichtlinie und der Erklärung des Zertifizierungsbetriebs.

LVR-InfoKom
Ottoplatz 2
50679 Köln
Deutschland

3.2 Kontaktpersonen

Folgende Personen sind Ansprechpartner für die Verwaltung der Zertifikatsrichtlinie und der Erklärung des Zertifizierungsbetriebs der LVR PKI G2:

Team IT Security Services
IT-Infrastruktur
LVR-InfoKom
Ottoplatz 2
50679 Köln
Deutschland
Tel.: +49 (221) 809-7650
Mail: trustcenter@lvr.de
Web: infokom.lvr.de

3.3 Verantwortliche Personen für das CPS

LVR-InfoKom ist verantwortlich für die Einhaltung des Zertifizierungsbetriebes und -richtlinien gemäß der CP/CPS und begleitender Dokumentation. Ansprechpartner zur Einhaltung der CP/CPS sind im Abschnitt 3.2 Kontaktpersonen aufgeführt.

3.4 CPS Genehmigungsverfahren

LVR-InfoKom ist verantwortlich für die Freigabe dieser CP/CPS. Die CP/CPS-Dokumentation wird fortwährend auf Konformität und Aktualität hin untersucht.

4 Publikationen und Informationsdienste

4.1 Verzeichnis- und Informationsdienste

Der Landschaftsverband Rheinland nutzt seinen Verzeichnisdienst für die Veröffentlichung der LVR G2 Root CA 01 Zertifikate. Für öffentliche Informationen, wie das LVR G2 Root CA 01 Zertifikat, CRLs und CP/CPS-Dokumentation, wird ein webbasierter Dienst als Informationsdienst genutzt.

4.2 Publikation von Zertifizierungsinformationen

Die Publikation der LVR PKI G2 Zertifikate erfolgt automatisiert durch den LVR Verzeichnisdienst. Hierzu ist keine Benutzerintervention ist notwendig.
Folgende Veröffentlichungsorte sind vorgesehen:

Zweck	**URL**
LVR PKI G2 CP und CPS	http://cps.pki.lvr.de/cps/LVR%20G2%20CPCPS.pdf
LVR Root CA 01 Zertifikat	http://aia.pki.lvr.de/aia/LVR%20G2%20Root%20CA%2001.crt
LVR Root CA 01 Sperrlisten	http://cdp.pki.lvr.de/cdp/LVR%20G2%20Root%20CA%2001.crl
LVR Sub CA 01 Zertifikat	http://aia.pki.lvr.de/aia/LVR%20G2%20Sub%20CA%2001.crt
LVR Sub CA 01 Sperrlisten	http://cdp.pki.lvr.de/cdp/LVR%20G2%20Sub%20CA%2001.crl
LVR Sub CA 01 Online Responder	http://ocsp.pki.lvr.de/ocsp
LVR Sub CA 02 Zertifikat	http://aia.pki.lvr.de/aia/LVR%20G2%20Sub%20CA%2002.crt
LVR Sub CA 02 Sperrlisten	http://cdp.pki.lvr.de/cdp/LVR%20G2%20Sub%20CA%2002.crl
LVR Sub CA 02 Online Responder	http://ocsp.pki.lvr.de/ocsp

Tabelle 1: Veröffentlichungsorte

4.3 Veröffentlichungsintervall

Die Veröffentlichung des LVR PKI G2 Zertifikatsrichtlinie und der Erklärung zum Zertifikatsbetriebs erfolgt jeweils nach ihrer Erstellung bzw. Aktualisierung.
Die Veröffentlichung der LVR PKI G2 Zertifikate erfolgt einmalig nach der Installation der der LVR PKI G2 Zertifizierungsstellen. Eine erneute Publikation erfolgt nur bei Ablauf bzw. Erneuerung der CA Zertifikats.
Sperrlisten (CRL) werden nach vorgeschriebenem Publikationsintervall erzeugt und sofort auf den PKI Web Diensten und in den LVR Verzeichnisdienst publiziert.

4.4 Zugang zu den Informationsdiensten

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

5 Identifikation und Authentifikation

5.1 Namen

5.1.1 Namensform

Der X.500 Distinguished Name in den CA-Zertifikaten für LVR Zertifikatsnehmer ist wie in die folgende Tabelle dargestellt, spezifiziert. Der Einsatz von DNs für die Benennung im Subject Name Field erlaubt die Eineindeutigkeit der Namensvergabe von Zertifizierungsstellen innerhalb des Landschaftsverbands Rheinland.
Das Schema für die Namensform ist bei allen ausgestellten Zertifikaten der LVR-InfoKom identisch und folgt untenstehendem Regelwerk:

CN = [Common Name],
OU = [Organization Unit],
O = [Organization],
L = [Locality],
S = [State or Province],
C = [Country],
E-Mail = [RFC822 Naming Context]

Die Attribute CN, O und C müssen genau einmal angegeben werden. In der tatsächlichen Umsetzung der Zertifizierungsstelleninfrastruktur werden nicht alle (Namens-) Attribute festgelegt, da die Aussagekraft und Eindeutigkeit der Namen für die Zertifizierungsstellen mit den dafür notwendigen Attributen als ausreichend erachtet wird. Die X.500 Distinguished Name laute:

LVR G2 Root CA 01	
Attribut	**Wert**
Common Name (CN)	LVR G2 Root CA 01
Organization	Landschaftsverband Rheinland
Country	DE
LVR G2 Sub CA 01	
Common Name (CN)	LVR G2 Sub CA 01
Organization	Landschaftsverband Rheinland
Country	DE
LVR G2 Sub CA 02	
Common Name (CN)	LVR G2 Sub CA 02
Organization	Landschaftsverband Rheinland
Country	DE

5.1.2 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.
- Der DN der LVR PKI G2 Zertifizierungsstellen wird durch die Namens-Objekte Common Name, Organisation, und Land gebildet. Eine Eindeutigkeit des DNs ist mit diesem zur Verfügung stehenden Namensobjekten zu gewährleisten.

- Sie Sub-CA Zertifikate wird durch die Namens-Objekte Common Name, Organisation, und Country gebildet. Eine Eindeutigkeit des DNs ist mit diesem zur Verfügung stehenden Namensobjekten zu gewährleisten. Die Verwendung von Organization Unit, Locality und State sind zulässig müssen jedoch nicht verwendet werden.

5.1.3 Anonymität und Pseudoanoymität von Zertifikatsnehmern

Anonyme Zertifikate oder Zertifikats die auf ein Pseudonym verweisen sind nicht zulässig.

5.1.4 Regeln zur Interpretation verschiedener Namensformen

Die ausgewiesenen Distinguished Name im Zertifikatsprofil folgen dem X.500 Standard.
Die LVR Email Adressen und UPN Einträge im Zertifikatsprofil folgen dem RFC 822 Regelwerk. UPN Namensinformationen müssen UTF-8 encodiert vorliegen.

5.1.5 Eindeutigkeit von Namen

Der komplette Distinguished Name in den von der LVR PKI G2 Zertifizierungsstellen ausgestellten Zertifikaten erlaubt die Eindeutigkeit von Namen der Zertifikatsnehmer.
Eine zusätzliche Kennung im alternativen Namensfeld, nämlich die eindeutige LVR E-Mail-Adresse, UPN Namen und Maschinen DNS Namen, sowie eine eindeutige Seriennummer in den Zertifikaten, berücksichtigt diesen Aspekt.
Die Verwendung von des '*' Zeichen im Namensfeld oder im alternativen Namensfeld ist nicht zulässig.

5.1.6 Erkennung, Authentifikation und Rolle von Warenzeichen

In der Regel beschränkt sich der DN Sub CA's und hat somit keine Relevanz in der Anerkennung von Warenzeichen. Grundsätzlich sind der Zertifikatsnehmer und auch der Zertifizierungsstellenbetreiber verpflichtet, aufgrund der automatisierten Ausstellung von End-Entitäten Zertifikaten, dass der Schutz von Warenzeichen gewährleistet wird.

5.2 Identitätsprüfung bei Neuantrag

5.2.1 Verfahren zur Überprüfung des Besitzes von privaten Schlüsseln

Die Schlüsselpaare der Zertifizierungsstellen der LVR PKI G2 werden auf der beantragenden Maschine generiert. Der Besitznachweis für die privaten Schlüssel 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.
Die Schlüsselpaare der Zertifizierungsstellen der LVR PKI G2 werden durch ein Hardware Security Modul generiert. 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.
Zertifikatsnehmer der LVR G2 Root CA 01 sind verpflichtet, privates Schlüsselmaterial durch ein Hardware Security Modul zu schützen, sofern diese im sogenannten Online Betrieb betrieben werden.
Zertifikatsnehmer der LVR G2 Sub CA 01 und LVR G2 Sub CA 02 sind verpflichtet, privates Schlüsselmaterial angemessen zu schützen. Die Verwendung von Software Speicher ist zulässig, sofern diese der angegebenen Zertifikatsnutzung entspricht.
Eine Überprüfung des privaten Schlüsselspeichers durch die LVR G2 Sub CA 01 bzw. LVR G2 Sub CA 02 (Key-Attestation) ist nicht vorgesehen. Der Zertifikatsnehmer garantiert durch die Teilnahme an der LVR PKI G2 den angemessenen Schutz der privaten Schlüssel.

5.2.2 Authentifikation der Organisation

Nichtzutreffend.

5.2.3 Authentifikation von Zertifikatsnehmern

Die Authentifikation von Zertifikatsnehmer der LVR PKI G2 erfolgt über das Personalwesen des Landesverband Rheinland oder alternativ über den LVR Verzeichnisdienst, welcher im Rahmen der LVR PKI als vollvertrauenswürdig definiert wurde

5.2.4 Nicht überprüfte Zertifikatsnehmer Information

Es werden nur die Informationen des Zertifikatsnehmers überprüft, welche notwendig sind in Rahmen der Authentifikation und Identifikation des Zertifikatsnehmers. Andere Informationen des Zertifikatsnehmers werden nicht berücksichtigt.

5.2.5 Prüfung der Berechtigung zur Antragstellung

Die Prüfung zur Berechtigen Antragstellung erfolgt durch die Validierung der Benutzer Identität im LVR Verzeichnisdienst.

5.2.6 Kriterien für Cross-Zertifizierung und Interoperation

Eine Cross-Zertifizierung mit anderen Organisationen ist nicht vorgesehen.

5.2.7 Identifikation und Authentifikation bei Zertifikatserneuerung

Die Identifizierung und Authentifizierung 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.

5.2.8 Identifikation und Authentifikation bei routinemäßiger Zertifikatserneuerung

Für die Erneuerung von Zertifikaten findet eine Identitätsprüfung durch die Registrierungsstelle statt. Identifikation und Authentifikation bei Zertifikatserneuerung nach erfolgtem Zertifikatsrückruf.

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

5.3 Identifikation und Authentifikation bei Zertifikatsrückruf

Der Zertifikatsrückruf erfolgt nur nach erfolgreicher Autorisierung oder dem LVR Incident Management. Die entsprechenden Prozesse für die Identifikation und Authentifikation beim Zertifikatsrückruf sind im Antragswesen beschrieben und niedergelegt. Grundsätzlich können LVR PKI G2 Zertifikatsnehmer die eigenen Zertifikate zurückziehen.

6 Betriebliche Anforderungen an den Zertifikatslebenszyklus

In der LVR PKI G2 können Teilnehmer gemäß Abschnitt 1.7 Zertifikate beantragen. Hierfür muss für ein Zertifikat eine Autorisierung vorliegen.

6.1 Zertifikatsantrag

Im vorangegangenen Abschnitt 4. sind die Rahmenbedingungen für die Zertifizierung zu entnehmen. Der Zertifikatsantrag für eine End-Identität erfolgt elektronisch im Zertifikatsmanagementsystem.
Weitergehende Informationen zum Zertifikatsantragsprozess können bei Bedarf bei der RA erfragt werden.

6.1.1 Antragsberechtigt für ein Zertifikat

Antragsberechtigt für ein Sub CA Zertifikat aus der sind:

Zertifizierungsinstanz	Berechtigter
LVR G2 Root CA 01	Betreiber von autorisierten LVR Sub CAs
LVR G2 Sub CA 01	Aktive Benutzer aus dem LVR Verzeichnisdienst.
LVR G2 Sub CA 02	Aktive Identität aus dem LVR Verzeichnisdienst.

6.1.2 Ausgabeprozess und Verantwortlichkeiten

Die Ausgabe eines Zertifikats erfolgt:

- an einen autorisierten Verantwortlichen in Form einer Datei im X.509 (CER) oder auf Wunsch im P7B (PKCS#7) Format
- an den Zertifikatsantragsteller
- über das Zertifikatsmanagementsystem

6.2 Prozess für die Antragsbearbeitung

6.2.1 Prozess für die Antragsbearbeitung für die LVR G2 Root CA 01

Der Zertifikatsnehmer hat die RA oder die Administration der LVR G2 Root CA 01 per Email über einen Zertifikatsantrag zu informieren. Der Antrag muss die Certification Policy (CP) der Sub CA hinzugefügt werden.

6.2.2 Prozess für die Antragsbearbeitung für die LVR G2 Sub CA 01 und LVR G2 Sub CA 02

Der Zertifikatsnehmer übergibt seinen Zertifikatsantrag elektronisch an das Zertifikatsmanagementsystem. Mit der Übertragung des Zertifikatsantrags garantiert der Antragsteller die Konformität seines Antrags mit der Zertifizierungsrichtlinie der LVR PKI G2.

6.2.3 Durchführung der Identifikation und Authentifizierung

Die Identifikation des Antragstellers erfolgt auf Basis eine aktivierten Benutzer Kontos im LVR Verzeichnisdienst.

6.2.4 Annahme oder Ablehnung von Zertifikatsanträgen

Die Annahme von Zertifikatsanträgen erfolgt auf Basis der Informationen der aktiven Benutzer / Antragstelle im LVR Verzeichnisdienst.
Die Ablehnung eines Zertifikatsantrags kann sowohl durch das Zertifikatsmanagementsystem sowie durch die LVR G2 Sub CA 01 oder LVR G2 Sub CA 02 erfolgen. Die Ablehnung von Zertifikatsanträge kann durch die Informationen im LVR Verzeichnisdienst automatisiert oder manuell erfolgen.
Es ist zulässig einen durch das Zertifikatsmanagementsystem angenommenen Antrag durch einen Zertifikatsmanager abzulehnen.
Automatisierte Annahme oder Ablehnungen von Zertifikatsanträgen müssen nicht durch die Zertifizierungsstellen kommentiert werden.
Antragsteller können Informationen zu einem Abgelehnten Zertifikatsantrag bei der jeweiligen Registrierungsstelle schriftlich erfragen.
Jeder Zertifikatsantrag wird mit einer eindeutigen Antragsnummer (Request-ID) versehen.

6.2.5 Verfahren zur Annahme von Zertifikatsanträge der Sub CAs

Die LVR G2 Sub CA 01 und LVR G2 Sub CA 02 unterstützt unterschiedliche Verfahren zur Annahme von Zertifikatsanträge.

6.2.6 Manuelle Zertifikatsanträge

Manuelle Zertifikatsanträge müssen in Form einer PKCS#10 Datei an die Registrierungsstelle per E-Mail übergeben werden. Der Zertifikatsantrag muss erklären, warum kein automatisierter Zertifikatsantrag an das Zertifikatsmanagement gestellt werden konnte (z.B. die Identität ist nicht im LVR Verzeichnisdienst vorhanden).
Zertifikatsinformationen die nicht über den LVR Verzeichnisdienst validiert werden können, müssen der Registrierungsstelle plausibel dargestellt werden. Im Zweifelsfall kann die Registrierungsstelle zusätzliche Autorisierungen vom Antragsteller anfordern.

6.2.7 Web basierte Zertifikatsanträge

Web basierte Zertifikatsanträge können über das Zertifikatsmanagementsystem gestellt werden. Der Zugang zum System kann über den LVR G2 PKI Betrieb erfragt werden.

6.2.8 Automatisierte Zertifikatsanträge

Zertifikatsanträge an die LVR G2 Sub CA 01 oder LVR G2 Sub CA 02 sind nur zulässig, wenn sämtliche Identitäten (Subject / SAN) innerhalb des Zertifikats eindeutig aus den Informationen aus dem LVR Verzeichnisdienst gebildet werden können.

6.2.9 http basierte Anträge

HTTP basierte Zertifikatsanträge können anhand von Zertifikats-Proxy-Diensten an die LVR G2 Sub CA 01 oder LVR G2 Sub CA 02 übergeben werden. Für HTTP basierte Anträge gelten die gleichen Bedingungen wie in 6.2.8.

6.2.10 Bearbeitungsdauer von Zertifikatsanträgen

Die Bearbeitungsdauer von Zertifikatsanträgen variiert basierend auf dem jeweiligen Anwendungsfall. Anträge werden ausschließlich zu den Bürozeiten des Landschaftsverbands Rheinland bearbeitet. Automatisierte Zertifikatsanträge, deren Validierung durch den LVR Verzeichnisdienst erfolgt, werden möglichst zeitnah verarbeitet. Die garantierte Bearbeitungsdauer für die jeweiligen Anwendungsfälle kann in den jeweiligen Prozessabläufen vom LVR G2 PKI Betrieb erfragt werden.

6.3 Zertifikatsausgabe

Die Zertifikatsausgabe für die LVR G2 Root CA 01 erfolgt per Email oder per Dateitransfer an den Antragsteller.

Die Zertifikatsausgabe für die LVR G2 Sub CA 01 und LVR G2 Sub CA 02 erfolgt durch das Zertifikatsmanagementsystem oder direkt durch die Zertifizierungsstelle anhand der im Kapitel 6.2 beschriebenen Antragsnummer. Die Zertifikatsausgabe erfordert eine Autorisierung im LVR Verzeichnisdienst

6.4 Zertifikatsannahme

Nichtzutreffend.

6.4.1 Verfahren der Zertifikatsannahme

Die formalen Voraussetzungen für die Ausstellung eines Zertifikats werden durch die CA in angemessener Weise überprüft. Insbesondere überprüft die LVR G2 Root CA 01 die Berechtigung des Teilnehmers für den im DN angegebenen Namen sowie die Gültigkeit der Signatur des Teilnehmermitarbeiters.
Ausgestellte Zertifikats der LVR G2 Sub CA 01 und LVR G2 Sub CA 02 werden über das Zertifikatsmanagementsystem zur Verfügung gestellt. Eine Annahme eines Zertifikats durch den Antragsteller ist nicht notwendig und nicht vorgesehen. Zertifikate die durch die LVR G2 Sub CA 01 oder LVR G2 Sub CA 02 signiert wurden gelten als gültig und benötigen keine Annahme durch den Antragssteller.

6.4.2 Publikation des Zertifikats

End-Entitäten Zertifikate werden nicht veröffentlicht. End-Entitäten Zertifikate für Verschlüsselung (z.B. S/MIME) werden LVR-Intern in den LVR Verzeichnisdienst veröffentlicht. Eine Publikation der Zertifikate außerhalb der LVR-InfoKom ist nicht vorgesehen.

6.4.3 Ausgabebenachrichtigung anderer Entitäten durch die CA

Eine Ausgabebenachrichtigung an andere Entitäten durch die Zertifizierungsstellen findet nicht statt.

6.4.4 Schlüsselpaar- und Zertifikatsverwendung

Private Schlüssel müssen angemessen in Hardware Security Module geschützt werden. Zertifikate dürfen ausschließlich in Übereinstimmung mit der Certification Policy (CP) der LVR PKI verwendet werden.

6.4.5 Nutzung des privaten Schlüssels und Zertifikats durch den Zertifikatsnehmer

Die Nutzung der Zertifikate durch den Zertifikatsnehmer hat den LVR Certification Policy (CP) zu folgen. In Kapitel 2 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.

6.4.6 Nutzung des privaten Schlüssels und Zertifikats durch vertrauende Parteien

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.

6.5 Zertifikatserneuerung

In Rahmen der LVR PKI G2 findet die Zertifikatserneuerung ausschließlich mit Schlüsselwechsel statt. Eine Zertifikatserneuerung mit gleichen Schlüsselpaaren, sprich ohne Schlüsselwechsel, ist nicht zulässig. Daher sind alle nachfolgenden Punkte unter 6.5 für die Zertifizierungsstelle der LVR G2 Root CA 01 nichtzutreffend.

6.5.1 Umstände für eine Zertifikatserneuerung

Eine Erneuerung von Zertifikaten erfolgt gemäß den Voraussetzungen für ein Zertifikat welche im Kapitel 6.1beschrieben sind.

6.5.2 Antragsberechtigte für eine Zertifikatserneuerung

Siehe Kapitel 6.1.

6.5.3 Durchführen einer Zertifikatserneuerung

Erfolgt den Vorgaben gemäß eines neuen Zertifikatsantrags. Siehe Kapitel 6.1.

6.5.4 Erneuerungsbenachrichtigung für den Zertifikatsnehmer

Eine Erneuerungsbenachrichtigung an den Zertifikatsbesitzer oder an Systeme die die Zertifikate zur Validierung von Benutzer oder Autorisierung von Programmen verwenden erfolgt nicht.

6.5.5 Verfahren zur Annahme der Zertifikatserneuerung

Nichtzutreffend.

6.5.6 Publikation des erneuerten Zertifikats durch die CA

Nichtzutreffend.

6.5.7 Erneuerungsbenachrichtigung anderer Entitäten durch die CA

Nichtzutreffend.

6.6 Zertifikatserneuerung mit Schlüsselwechsel

In Rahmen der LVR PKI G2 findet die Zertifikatserneuerung ausschließlich mit Schlüsselwechsel statt. Technisch betrachtet handelt es sich um die Ersetzung eines Zertifikates durch ein Zertifikat mit neuer Gültigkeitsdauer und für ein neues Schlüsselpaar aber sonst unveränderten Zertifikatsinhalten.

6.6.1 Umstände für eine Zertifikatserneuerung mit Schlüsselwechsel

Die Zertifikatserneuerung mit Schlüsselwechsel kann beantragt werden, wenn einer der folgenden Voraussetzungen erfüllt sind:

- die Hälfte der Gültigkeitsdauer des aktuellen Zertifikats ist abgelaufen oder steht kurz vor Ablauf
- die im Zertifikat enthaltenen Daten sind nicht korrekt.
- der alte Schlüssel kann oder darf nicht mehr verwendet werden, weil er (möglicherweise) kompromittiert wurde
- die Gültigkeitsdauer des aktuellen Zertifikats oder die aktuelle Schlüssellänge bietet keine ausreichende Sicherheit mehr

6.6.2 Antragsberechtigte für eine Zertifikatserneuerung mit Schlüsselwechsel

Sind alle Zertifikatsnehmer, denen ein gültiges Zertifikat durch die LVR PKI G2 zugewiesen wurde

6.6.3 Durchführen einer Zertifikatserneuerung mit Schlüsselwechsel

Der Prozess erfolgt technisch analog der Erstantragsstellung.

6.6.4 Erneuerungsbenachrichtigung für den Zertifikatsnehmer

Es erfolgt keine Erneuerungsbenachrichtigung für auslaufende Zertifikate.

6.6.5 Verfahren zur Annahme der Zertifikatserneuerung mit Schlüsselwechsel

Das Verfahren für eine Zertifikatserneuerung folgt den Richtlinien eines Zertifikatsneuantrags.

6.6.6 Publikation des erneuerten Zertifikats durch die CA

Zertifikate werden auch nach einer Erneuerung nicht veröffentlicht.

6.6.7 Erneuerungsbenachrichtigung anderer Entitäten durch die CA

Eine Ausgabebenachrichtigung an andere Entitäten findet nicht statt.

6.7 Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

In Rahmen der LVR PKI G2 findet die Zertifikatserneuerung ausschließlich mit Schlüsselwechsel statt. Eine Anpassung der Zertifikatsinhalte (Datenanpassung) ist nicht zulässig und wird über eine Neubeantragung ausgeführt. Daher sind alle nachfolgenden Punkte unter 6.7 für die LVR PKI G2 nichtzutreffend.

6.7.1 Umstände für eine Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Nichtzutreffend.

6.7.2 Antragsberechtigte für eine Zertifikatserneuerung mit Schlüsselwechsel

Nichtzutreffend.

6.7.3 Durchführen einer Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Nichtzutreffend.

6.7.4 Erneuerungsbenachrichtigung für den Zertifikatsnehmer

Nichtzutreffend.

6.7.5 Verfahren zur Annahme der Zertifikatserneuerung mit Schlüsselwechsel mit Datenanpassung

Nichtzutreffend.

6.7.6 Publikation des erneuerten Zertifikats durch die CA

Nichtzutreffend.

6.7.7 Erneuerungsbenachrichtigung anderer Entitäten durch die CA

Nichtzutreffend.

6.8 Zertifikatssperrung und -suspendierung

Eine Suspendierung von Zertifikaten ist nicht vorgesehen.

6.8.1 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 der Eigentümer sein Zertifikat nicht mehr nutzen kann, z.B. es keinen Zugriff auf das Schlüsselmaterial mehr existiert.
- Wenn zu dem Zertifikat, eine Zertifikatserneuerung mit Schlüsselwechsel beantragt wurde oder in Kürze beantragt wird.
- Wenn Sub CA ihre Zertifizierungsdienste eingestellt. In diesem Fall werden sämtliche von den Zertifizierungsdiensten ausgestellten Zertifikate gesperrt.
- Die Zertifikate sind zu sperren, wenn der Zertifikatseigentümer die Voraussetzungen für die Verwendung des Zertifikates nicht mehr erfüllt, z.B., weil bestehende Zertifikatsrichtlinie verstoßen wird.

6.8.2 Antragsberechtigte für eine Sperrung

Folgende Personenkreise und Instanzen sind berechtigt Zertifikate zu sperren:

- die Sperrung von Benutzerzertifikaten Zertifikat kann durch
    - den Zertifikatsnehmer selbst (Zertifikatsinhaber/-nehmer)
    - seinen Vertreter (durch Vollmacht)
    - seinen Vorgesetzten oder
    - durch den LVR Registrierungsstellenmitarbeiter veranlasst werden.
- Die Sperrung von CA Zertifikaten kann durch die Leitung der LVR Zertifizierungsstellen veranlasst werden.

6.8.3 Durchführung einer Zertifikatssperrung

Die Zertifikatssperrung erfolgt über einen schriftlichen Antrag. Der Antrag ist an ISC@lvr.de zu richten. Ein Ticket wird für die zugewiesene Registrierungsstelle generiert. Eine sofortige Sperrung, kann nur durch den LVR Sicherheitsbeauftragen bzw. durch dessen Stellvertreter angewiesen werden. Durchgeführt wird die Zertifikatssperrung grundsätzlich durch die Registrierungsstelle der jeweiligen Zertifizierungsstelle.

6.8.4 Meldefrist von Sperranträgen für Zertifikatsnehmer

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

6.8.5 Bearbeitungsdauer von Sperranträgen durch die CA

Sperranträge werden innerhalb eines Arbeitstages zu den LVR Service Zeiten durchgeführt.

6.8.6 Prüfung des Zertifikatsstatus durch vertrauende Parteien

Eine Überprüfung des Zertifikatsstatus durch vertrauende Parteien wird empfohlen. Der Die aktuellen Zertifikatssperrlisten können durch die in die im Zertifikat enthaltenen CDPs (CRL Distribution Points) heruntergeladen werden.

6.8.7 Ausstellungszeiträume für CRLs

- Der Ausstellungszeitraum für eine Sperrliste der LVR G2 Root CA 01 beträgt: 4 Monate
- Der Standardveröffentlichungszeitraum für eine Sperrliste der LVR G2 Root CA 01 (Überlappungsperiode) beträgt 1 Monat
- Für die LVR G2 Sub CA 01 und LVR G2 Sub CA 02 gelten folgende Veröffentlichungszeiträume
    - LDAP Veröffentlichungspfad:
        - Basis CRL beträgt 10 Tage (7 Tage Veröffentlichungszeitraum plus 3 Tage Überlappungszeitraum)
        - Delta CRL beträgt 6 Stunden (4 Stunden Veröffentlichungszeitraum plus 2 Stunden Überlappungszeitraum
    - http Veröffentlichungspfad:
        - Basis CRL beträgt 10 Tage (7 Tage Veröffentlichungszeitraum plus 3 Tage Überlappungszeitraum)
        - Delta CRL beträgt 6 Stunden (4 Stunden Veröffentlichungszeitraum plus 2 Stunden Überlappungszeitraum

Der LDAP Veröffentlichungspfad wird nicht in den ausgegebenen Zertifikaten referenziert und ist von außen nicht erreichbar. Delta Sperrlisten werden ausschließlich als technische Sperrlisten verwendet und sind nicht in der Basis-Sperrliste oder Zertifikat referenziert.

6.8.8 CRL Veröffentlichung nach Sperrung

Sollte ein Zertifikat gesperrt werden, wird eine aktualisierte Sperrliste umgehend veröffentlicht.

6.8.9 Maximale Latenz von CRLs

Die CRLs stehen sofort nach Veröffentlichung auf den LVR PKI Web-Servern zur Verfügung.

6.8.10 Online Sperrung und Statusprüfung von Zertifikaten

Die LVR G2 Root CA 01 verwendet keine Online Sperrlisten. Die LVR G2 Sub CA 01 und LVR G2 Sub CA 02 verwendet Online Sperrlisten über das Online Certificate Status Protocol (OCSP) gemäß dem RFC 6960. Das Zertifikat für die Signatur einer Online Zertifikats Statusanfrage ist gemäß RFC6960.
Das OCSP Signatur Zertifikat enthält keine Sperrinformationen gemäß RFC 6960. Die Nichtverwendung von Sperrinformation wird über die Zertifikatserweiterung 1.3.6.1.5.5.7.3.9 bekannt gegeben.
Die Online Sperrsysteme verwenden ausschließlich HSM geschützte Schlüssel zur Signierung von Sperranfragen.
Die Verwendung von Online Sperrungen von Zertifikaten obliegt dem Zertifikatsnehmer bzw. dem Zertifikatsüberprüfenden System.

6.8.11 Anforderung für die Online Prüfung des Sperrstatus

Für die Verwendung der Online Sperrüberprüfung muss ein RFC 6069 kompatibler RFC Resolver verwendet werden.

6.8.12 Informationen für die Online Prüfung des Sperrstatus

Die von der LVR G2 Sub CA 01 und LVR G2 Sub CA 02 signierten Zertifikaten werden mit den Informationen der Online Sperrserver versehen.

6.8.13 Weitere Arten zur Bekanntmachung von Zertifikatsstatus

Es sind keine weiteren Arten zur Bekanntmachung des Zertifikatsstatus vorgesehen. Die Sperrlisten werden auf Web-Servern und im Verzeichnisdienst veröffentlicht. Die Veröffentlichung über den Web Server werden über die CDP Einträge bekannt gemacht werden.

6.8.14 Spezielle Maßnahmen bei Schlüssel-Kompromittierung

Bei einem Hinweis einer Schlüssel-Kompromittierung wird eine sofortige Untersuchung durchgeführt. Sollte die Kompromittierung sich als stichhaltig erweisen, so werden die notwendigen Maßnahmen ergriffen, wie die Sperrung der betroffenen Zertifikate.

6.8.15 Umstände für eine Suspendierung

Eine Suspendierung von Zertifikaten ist ausschließlich für SmartCard Zertifikate vorgesehen. Für alle anderen Zertifikate ist eine Suspendierung nicht vorgesehen.

6.8.16 Berechtigte für eine Suspendierung

SmartCard Zertifikate können durch das Zertifikatsmanagementsystem suspendiert werden. Für alle anderen Zertifikate ist eine Suspendierung nicht vorgesehen.

6.8.17 Durchführung einer Suspendierung

Die Suspendierung von SmartCard Zertifikaten erfolgt ausschließlich über das Zertifikatsmanagementsystem.

6.8.18 Dauer einer Suspendierung

Die Suspendierung eines SmartCard Zertifikats beträgt maximal einen Werktag. Danach muss das Zertifikat endgültig zurückgezogen werden.

6.9 Auskunftsdienste für den Zertifikatsstatus

LVR-InfoKom betreibt einen Auskunftsdienst über den Zertifikatsstatus. Dieser Auskunftsdienst ist web-basiert und alternativ über LDAP erreichbar. Es werden die CRLs (Zertifikatssperrlisten) veröffentlicht. Der LDAP Verteilpunkt ist nur intern zugänglich und wird in den ausgestellten Zertifikaten nicht referenziert.

6.9.1 Betriebliche Ausprägung

Der Auskunftsdienst basiert auf den LVR PKI Web Server und verwendet als Übertragungsprotokoll http. Auf folgenden URI können die CRLs der Zertifizierungsstellen der LVR PKI G2 über die im Kapitel 4.2 angegebenen Pfade abgerufen werden:
http://www.pki.lvr.de

Die CRLs und zu sperrende Zertifikate müssen von der jeweiligen Zertifizierungsstelle der LVR PKI G2 ausgegeben worden sein. Eine Unterstützung von „indirekten CRLS" ist nicht gegeben.
Das ausgegebene CRL Profil ist zum RFC 5280 konform und entspricht dem X.509 Version 2 Standard.

6.9.2 Verfügbarkeit des Auskunftsdienstes

Die Verfügbarkeit der LVR PKI Web-Server und LVR Verzeichnisdienst ist für einen 7 x 24h Betrieb ausgelegt.

6.9.3 Optionale Funktionen

Nichtzutreffend.

6.10 Beendigung des Vertragsverhältnisses durch den Zertifikatsnehmer

Ein Eigentümer oder Zertifikatsnehmer eines LVR PKI G2 Zertifikats scheidet aus den Zertifizierungsdiensten aus, wenn das Zertifikat nicht mehr benötigt wird oder eine Kompromittierung des Zertifikats vorliegt.

6.10.1 Schlüsselhinterlegung und -wiederherstellung

Eine Schlüsselhinterlegung und –wiederherstellung wird nicht unterstützt.

6.10.2 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

Nichtzutreffend.

6.10.3 Richtlinien und Praktiken zur Hinterlegung und Wiederherstellung von Sitzungsschlüsseln (symmetrischen Schlüsseln)

Nichtzutreffend.

7 Einrichtungen, Sicherheitsmanagement, organisatorische und betriebliche Sicherheitsmaßnahmen

7.1 Physikalische- und Umgebungssicherheit

Die infrastrukturellen Sicherheitsmaßnahmen der LVR PKI G2 Zertifizierungsstellen sind im LVR-InfoKom Rechenzentrumsbetrieb eingebunden. Die Zertifizierungsstellen der LVR PKI G2 sind virtuelle Maschinen die auf einem Hyper-Visor gemäß den Sicherheitsvorgaben der LVR-InfoKom betrieben wird. Folgende Vorkehrungen und physikalische Schutzmaßnahmen sind integraler Bestandteil der Rechenzentren betrieben durch die LVR-InfoKom.

7.1.1 Lage und Konstruktion

Die Hyper-Visor für den Betrieb der Zertifizierungsstellen der LVR PKI G2 befinden sich in den Räumlichkeiten der LVR-Rechenzentrums. Die Räume bieten hinsichtlich der physikalischen Sicherheitsmaßnahmen einen ausreichenden Schutz, der dem erforderlichen Sicherheitsniveau angemessen ist.

7.1.2 Zutrittskontrolle

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

7.1.3 Stromversorgung und Klimatisierung

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

7.1.4 Wasserschäden

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

7.1.5 Prävention und Schutz vor Feuer

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

7.1.6 Datenträger

Es werden folgende Datenträger verwendet:

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

Datenträger werden in verschlossenen Schränken aufbewahrt. Datenträger mit sensiblen Daten, wie z. B. HSM Hardware Tokens, werden in einem Tresor aufbewahrt.

7.1.7 Abfall Entsorgung

Informationen auf elektronischen Datenträgern werden sachgemäß vernichtet und anschließend sachgerecht entsorgt. Papierdatenträger werden mittels vorhandenen Aktenvernichtern zerstört und sachgerecht entsorgt.

7.1.8 Off-site Backup

Der LVR-Rechenzentrumsbetrieb regelt die Anlage für Off-Site Sicherungen.

7.2 Organisatorische Sicherheitskontrollen

7.2.1 Sicherheitskritische Rollen

Sicherheitskritische Aufgaben werden für den Betrieb der LVR PKI G2 in Rollen zusammengefasst. Ein Rollenkonzept ist verfügbar und wird für den organisatorischen Prozess und auch für den HSM (Hardware Security Module) Betrieb umgesetzt.
Für den Betrieb der LVR G2 Sub CA 01 und LVR G2 Sub CA 02 sind folgende Rollen vorgesehen:

- CA Administration
  - Management des CA Server
  - Management des CA Dienstes
  - Management der CA Konfiguration
  - CA Sicherungs- und Wiederherstellungsmanagement
- HSM Administration
  - Management der HSM
  - HSM Sicherungs- und Wiederherstellungsmanagement
- Zertifikatsadministration
  - Bearbeiten von Zertifikatsanträge
  - Bearbeiten von Sperranträgen

Eine Detaillierte Beschreibung der Rollendefinition kann bei Bedarf von der IT-Infrastruktur erfragt werden.

7.2.2 Zugewiesene Zahl von Personen bei sicherheitskritischen Aufgaben

Das Vier-Augen-Prinzip gilt beifolgenden Operationen:

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

7.2.3 Identifikation und Authentifikation der Rollen

Die Identifikation und Authentisierung 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 von Zertifizierungsstellen-schlüssel wird das Vier-Augen-Prinzip adressiert.

7.2.4 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

7.3 Sicherheitsmaßnahmen für das Personal

LVR-InfoKom stellt in Rahmen der LVR PKI G2 erfahrenes Personal zur Verfügung. Notwendige Qualifikation, Wissenstand und Erfahrungswerte des Personals sind für den sicheren PKI Regelbetrieb vorhanden.

7.3.1 Anforderung an Qualifikation, Erfahrung und Freigabestufe

Das zuständige Personal verfügt über die erforderlichen spezifischen Kenntnisse und Erfahrungen aus dem Bereich der X.509 PKI und dem notwendigen Systembetrieb.

7.3.2 Prozess zur Sicherheitsüberprüfung von Mitarbeitern

Es gelten die allgemeinen Personaleinstellungsrichtlinien des LVR.

7.3.3 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.

7.3.4 Trainingsfrequenz

Die Frequenz der Trainings orientiert sich an den Anforderungen der LVR PKI G2. Trainings werden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und Sicherheitstechnik durchgeführt.

7.3.5 Frequenz und Abfolge von Job Rotation

Eine Job Rotation ist nicht vorgesehen.

7.3.6 Sanktionen bei unzulässigen Handlungen

Die allgemeinen Sanktionsmöglichkeiten der LVR-InfoKom werden bei unzulässigen Handlungen angewandt.

7.3.7 Vertragsbedingungen für das Personal

Das LVR PKI G2 Betriebspersonal verpflichtet sich auf die die Einhaltung von Anweisungen und gesetzlichen Vorschriften. Diese beinhalten insbesondere eine Verpflichtung, personenbezogene Daten vertraulich zu behandeln.

7.3.8 An das Personal ausgehändigte Dokumente

Folgende Dokumente werden dem LVR Personal zum ordnungsgemäßen Betrieb der LVR PKI G2 zur Verfügung gestellt:

- Zertifikatsrichtlinie oder Certificate Policy (CP)
- Erklärung zum Zertifizierungsbetrieb oder Certification Practice Statement (CPS)
- Betriebskonzept und Sicherheitskonzept der Zertifizierungsinstanzen der LVR PKI G2
- Handlungsanweisungen
- Betriebshandbücher der Systeme und Software

7.4 Überwachung von sicherheitskritischen Ereignissen

7.4.1 Protokollierte Ereignisse

Zu jedem Ereignis werden folgenden Daten erfasst:

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

Die folgenden Ereignisse werden elektronisch protokolliert:

- Ereignisse im Lebenszyklus von Zertifikaten/Smartcards und Schlüsselpaare:
    - Ausstellung von Zertifikaten
    - Veröffentlichung von Zertifikaten
    - Registrierung für eine Erneuerung von Zertifikaten
    - Sperranfragen an die CA durch die RA
    - Sperrungen
    - Erstellung von Sperrlisten
- Ereignisse im Lebenszyklus der Verschlüsselungsschlüsselpaare:
    - Generierung von Verschlüsselungsschlüsselpaaren
    - Archivierung (Backup) von privaten Verschlüsselungsschlüsseln
    - Wiederherstellung von privaten Verschlüsselungsschlüsseln
- Systemereignisse und Fehlermeldungen der sicherheitskritischen Systeme:
    - Versuche zur An- und Abmeldung
    - Vergabe und Entzug von Zugriffsberechtigungen
    - Zugriffe und Zugriffsversuche per Netzwerk
- Ereignisse der Zutrittskontrollanlagen:
    - Betreten und Verlassen von gesicherten Räumen
    - Fehlgeschlagene Zutrittsversuche und Alarme
    - Vergabe und Entzug von Zutrittsberechtigungen
    - Beantragung, Ausgabe und Sperrung von Zutrittskarten

Ergänzend zu den elektronischen Log-Dateien werden auch Änderungen der Richtlinien und des Betriebshandbuchs erfasst:

- Rollendefinitionen
- Prozessbeschreibungen
- Wechsel der Verantwortlichkeiten

7.4.2 Überprüfungshäufigkeit von Log-Daten

Bei Verdacht auf Unregelmäßigkeiten wird eine umgehende Prüfung veranlasst.

7.4.3 Aufbewahrungsfristen von Audit Log-Daten

Sicherheitsrelevante Protokolldaten werden entsprechend den gesetzlichen Regelungen aufbewahrt.

7.4.4 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 zugänglich.

7.4.5 Audit Log-Daten Backup-Verfahren

Die Protokolldaten werden zusammen mit anderen relevanten Daten der LVR G2 Root CA 01 einem regelmäßigen Backup unterzogen.

7.4.6 Audit Collection System (Protokollierungssystem intern oder extern)

Nichtzutreffend.

7.4.7 Benachrichtigung bei Auslösen eines sicherheitskritischen Ereignisses

Eine Benachrichtigung des LVR G2 Root CA 01 Bedienerpersonals über E-Mail findet bei Auftreten von sicherheitskritischen Ereignissen statt.

7.5 Archivierung von Protokolldaten

LVR-InfoKom archiviert in Rahmen des PKI Betriebes die notwendigen Protokolldaten.

7.5.1 Archivierte Protokolldatentypen

Archiviert werden Daten, die für den Zertifizierungsprozess relevant sind:

- Zertifikatanträge, diese enthalten persönliche Daten des Zertifikatnehmers
- Alle von der Zertifizierungsstelle ausgestellten Zertifikate
- Sperranträge für Verschlüsselung/Signatur Zertifikate und für Zertifizierungsstellen Zertifikate
- Sperrlisten (Certificate Revocation Lists CRLs)
- Dokumentationen von Prozeduren und Systemen (z.B. Handlungsanweisungen, Notfallpläne, Systemhandbücher)
- Protokolle von sicherheitsrelevanten interner Prozeduren und Prozesse:
    - Prozeduren der Schlüsselzeremonie
    - Prozeduren bei Installation und Konfiguration der Zertifizierungsstellen
    - Prozeduren bei Installation und Konfiguration des Personen PKIs
    - 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

7.5.2 Archivierungsfristen

7.5.3 Nichtzutreffend.Schutzmaßnahmen für das Archiv

Es wird durch geeignete Maßnahmen sichergestellt, dass die Daten nicht verändert oder gelöscht werden können. Es wird darüber hinaus sichergestellt, dass die Daten nicht unbefugt gelesen oder kopiert werden können.
Die Schutzmaßnahmen für elektronische Datenträger entsprechen den für den Rechenzentrumsbetrieb der LVR-InfoKom vorgesehenen Prozessen:

- Nur das verantwortliche Personal für das Archiv erhalten Zutritt zum Archiv.
- Die Archive sind durch Klimaanlagen und Vorrichtigen zum Brandschutz vor Umwelteinflüssen geschützt.
- LVR-InfoKom ist verantwortlich für die Übertragung der archivierten elektronischen Daten im Fall einer Technologieablösung auf aktuelle Datenträgertypen.

7.6 Schlüsselwechsel der Zertifizierungsstellen

Bei einem Schlüsselwechsel der LVR PKI G2 Zertifizierungsinstanzen wird das aktuelle CA Zertifikat durch ein neues, im Falle der LVG G2 Root CA 01 selbst-signiertes, Zertifikat ersetzt und veröffentlicht. Eine Sperrung der selbst-signierenden Root CA Zertifikats ist technisch auf der CA Seite nicht machbar. Für die LVR G2 Sub CA 01 und LVR G2 Sub CA 02 erfolgt eine Sperrung des Zertifikats nur bei einer Kompromittierung. Der Schlüsselwechsel ist für jede CA nach der Hälfte der Zertifikatslaufzeit geplant.

7.7 Kompromittierung und Wiederanlauf nach Katastrophen

7.7.1 Prozeduren bei Sicherheitsvorfällen und Kompromittierung

Es existieren Notfallpläne der LVR-InfoKom, 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.

7.7.2 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.

7.7.3 Wiederanlauf bei Kompromittierung von privaten Schlüsselmaterial

Die Kompromittierung von privatem Schlüsselmaterial stellt einen ernstzunehmenden Zwischenfall 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 LVR Benutzerzertifikats wird das jeweilige Zertifikat sofort gesperrt.
- Bei Kompromittierung von privatem Schlüsselmaterial der LVR Maschinenzertifikate werden Zertifikate mit neuem Schlüsselmaterial ausgegeben. Eine Sperrung der kompromittierten Zertifikate ist beim LVR noch in der Diskussion.
- 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 diese in Rahmen des Anwendungsprofils tatsächlich genutzt wird.

7.7.4 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.

7.7.5 Einstellung des Betriebs der Zertifizierungs- und/oder Registrierungsstelle

Im Falle der Einstellung des Betriebes der LVR-InfoKom Zertifizierungsstellen oder der Registrierungsstellen sind folgende Maßnahmen festgelegt:

- Alle Zertifikatsnehmer und vertrauende Parteien werden von der Einstellung des Zertifizierungsdienstes informiert. Mindestfrist von einem Monat vor Einstellung wird angedacht.
- Alle LVR Benutzerzertifikate, sowie die Zertifikate der Zertifizierungsstellen werden gesperrt.
- Alle privaten Schlüssel der Zertifizierungsstellen und der LVR Benutzerzertifikate der Zertifikatsnehmer werden vernichtet.
- Ausnahme bildet das Schlüsselmaterial für die Verschlüsselung. Diese werden in gesicherten Umgebungen, z. B. verschlüsselte Datenbank, archiviert.

8 Technische Sicherheitsmaßnahmen

8.1 Schlüsselpaarerzeugung und Installation

8.1.1 Schlüsselpaarerzeugung

Die Schlüsselerzeugung und die Auswahl der Crypto-Algorithmen für die LVR G2 Root CA 01 erfolgt nach FIPS 140-2 Level 1 bzw. 3 (Federal Information Processing Standards).
Die Generierung der Schlüsselpaare wird von Hard- und Softwarekomponenten ausgeführt und unterscheidet sich je nach Entität:

Schlüsselpaargenerierung für die LVR Zertifizierungsstellen:

Alle Schlüsselpaare für die LVR Zertifizierungsstellen werden durch das Netzwerk-HSM (Hardware Security Modul) generiert. Die generierten CA Schlüssel werden auch durch das Netzwerk HSM kryptographisch geschützt. Jeglicher Prozess, der den Zugriff auf den privaten Schlüssel der Zertifizierungsstelle erforderlich macht, ist das HSM zwingend eingebunden. Das LVR Netzwerk HSM wird im Fips 140-2 Level 3 Modus betrieben.

8.1.2 Auslieferung der privaten Schlüssel an Zertifikatsnehmer

Private Schlüssel der LVR Zertifizierungsstellen:

Jeglicher Prozess, der den Zugriff auf den privaten Schlüssel der Zertifizierungsstelle erforderlich macht, ist das HSM zwingend eingebunden; alle privaten CA Schlüssel liegen nur in der HSM selbst vor.
Eine Auslieferung des privaten Schlüsselmaterials von CA Schlüsseln ist nicht notwendig, da die HSM für die Schlüsselerzeugung und als sichere Ablage für private Schlüssel dient.

8.1.3 Auslieferung der öffentlichen Schlüssel an Zertifikatsaussteller

Der Certificate Signing Request (CSR) des Zertifikatnehmers wird in PKCS#10 Format übermittelt. Der gesamte Prozess rein manuell statt.

8.1.4 Auslieferung der öffentlichen CA Schlüsseln anvertrauende Parteien

Die Auslieferung der öffentlichen CA Schlüsseln erfolgt manuell über die dafür vorgesehenen Web-URLs geladen werden:

Zertifizierungs-instanz	Veröffentlichungspfad
LVR G2 Root CA 01	http://aia.pki.lvr.de/aia/LVR%20G2%20Root%20CA%2001.crt
LVR G2 Sub CA 01	http://aia.pki.lvr.de/aia/LVR%20G2%20Sub%20CA%2001.crt
LVR G2 Sub CA 02	http://aia.pki.lvr.de/aia/LVR%20G2%20Sub%20CA%2002.crt

8.1.5 Schlüssellängen

Detailinformationen sind dem aktuellen LVR RFC 5280 Zertifikatsprofiltabelle zu entnehmen

LVR G2 Root CA 01 Schlüssellänge:

LVR Root CA – 4096bit (HSM) – RSA Algorithmus

LVR G2 Sub CA 01 Schlüssellänge:

LVR Root CA – 4096bit (HSM) – RSA Algorithmus

LVR G2 Sub CA 02 Schlüssellänge:

LVR Root CA – 4096bit (HSM) – RSA Algorithmus

8.1.6 Erzeugung und Prüfung der Schlüsselparameter

Für den RSA Algorithmus nichtzutreffend.

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

Siehe auch Kapitel 9.

LVR CA Schlüsselverwendung:

Certificate Signing, Offline CRL Signing, CRL Signing (06).

8.1.8 Schutz des privaten Schlüssels und kryptographische Module

In der LVR PKI G2 wird privates Schlüsselmaterial durch kryptographische Module in der Ausprägung als Hardware geschützt.

8.1.9 Standards und Sicherheitsmaßnahmen von kryptographischen Modulen

Das eingesetzte Netzwerk HSM ist nach FIPS 140-2, Level 2 und Level 3 evaluiert.

8.1.10 Mehr-Personenkontrolle von privaten Schlüsseln (n von m Verfahren)

Eine Schlüsselteilung von privaten Schlüsseln findet nicht statt. Ausnahme bildet der Betrieb der Netzwerk HSM. Ein n-von-m Verfahren für die HSM Verwaltung wurde eingerichtet.

8.1.11 Hinterlegung von privaten Schlüsseln

Nichtzutreffend.

8.1.12 Backup von privaten Schlüsseln

Privates Schlüsselmaterial der LVR PKI G2 Zertifizierungsstellen wird durch die Netzwerk HSM eigenen Backup Komponenten und Prozesse gesichert. Archiviertes privates Schlüsselmaterial wird durch verfügbare Backup Methoden gesichert.

8.1.13 Archivierung von privaten Schlüsseln

Nichtzutreffend.

8.1.14 Transfer von privaten Schlüsseln in oder aus einem kryptographischen Modul

Nichtzutreffend. Ein Transfer von privaten Schlüsseln ist nicht vorgesehen, da alle privaten Schlüssel in der Komponente verbleiben, die diese auch erzeugt haben.

8.1.15 Ablage von privaten Schlüsseln im kryptographischen Modul

Die privaten Schlüssel der LVR PKI G2 wird ausschließlich in den Netzwerk HSM der Zertifizierungsdienste gespeichert.

8.1.16 Aktivierung der privaten Schlüssel

Nichtzutreffend.

8.1.17 Deaktivierung der privaten Schlüssel

Nichtzutreffend. Eine Deaktivierung von privaten Schlüsseln ist nicht vorgesehen.

8.1.18 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 in HSMs gespeichert werden, werden durch das Löschen des Schlüssels im HSM vernichtet.

8.1.19 Bewertung des kryptographischen Moduls

Das eingesetzte Netzwerk HSM wird nach FIPS 140-2, Level 3 betrieben.
Die eingesetzten Software Crypto-Module werden nach FIPS 140-2, Level 1 betrieben.

8.2 Weitere Aspekte für die Verwaltung von Schlüsselpaaren

8.2.1 Archivierung der öffentlichen Schlüssel

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

8.2.2 Gültigkeit von Zertifikaten und Schlüsselpaaren.

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

Zertifizierungsinstanz	Maximale Gültigkeit der ausgestellten Zertifikate
LVR G2 Root CA 01	7 Jahre
LVR G2 Sub CA 01	2 Jahre
LVR G2 Sub CA 02	2 Jahre

8.2.3 Aktivierungsdaten

Nichtzutreffend.

8.3 Sicherheitsmaßnahmen für Computer

8.3.1 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.
- 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.
- Auf den dürfen Systemen nur nach Maleware 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.

8.3.2 Bewertung der Computersicherheit

Die LVR PKI G2 baut auf Zertifizierungsdiensten auf, die nach Common Criteria EAL (Evaluation Assurance Level) 4+ (FLR – augmented with Flow Remediation) evaluiert sind.
Das eingesetzte Netzwerk HSM ist nach FIPS 140-2, Level 2 and Level 3 validiert.

8.4 Technische Kontrollen für den gesamten Lebenszyklus

8.4.1 Sicherheitsmaßnahmen bei der Systementwicklung

Nichtzutreffend.

8.5 Sicherheitsmanagement

Das Sicherheitsmanagement der Zertifizierungsinstanzen der LVR PKI G2 muss den Vorgaben der LVR-InfoKom entsprechen. Das Betriebssystem der Zertifizierungsinstanzen der LVR PKI G2 wird regelmäßig, spätestens 3 Monate nach der Veröffentlichung der LVR-InfoKom definierten Sicherheitsstandards angepasst.

8.5.1 Sicherheitsmaßnahmen für den gesamten Lebenszyklus

In Rahmen des Sicherheitskonzeptes für das LVR PKI G2 und die zugehörigen Zertifizierungsstellen werden die notwendigen Sicherheitsmaßnahmen beleuchtet. Detailinformation zum Sicherheitskonzept können bei Bedarf von der IT-Infrastruktur erfragt werden.

8.5.2 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.

8.6 Zeitstempel

Die LVR 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 dem LVR Verzeichnisdienst automatisch synchronisiert. Die Zeitsynchronisation der LVR Root CA erfolgt manuell.
Der Einsatz einer vertrauenswürdigen und evaluierten Zeitstempelkomponente ist für die LVR PKI G2 Lösung nicht vorgesehen.

9 Zertifikats- und CRL Profil

In Rahmen der X.509 PKI sind Zertifikats- und CRL Profile für die LVR G2 Root CA 01 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.

9.1 Zertifikatsprofil

LVR G2 Root CA 01 entspricht:

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

LVR Zertifikatsprofile sind konform:

- RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 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

Die Basisbeschreibung von LVR Zertifikaten enthält:

Feld	**Wert**
Version	Siehe auch 9.1.1*Version Numbers(s)*
Serial Number	Unique value in the namespace of each CA
Signature Algorithm	Designation of algorithm used to sign the certificate. Siehe auch 9.1.3 *Algorithm Object Identifiers*
Issuer	siehe auch 9.1.4 *Name Forms*
Validity	Validity (from and to) time and date information.’
Subject	siehe auch 9.1.4 *Name Forms*
Subject Public Key	Zugehöriger Public Key
Signature	CAs signature
Certificate Policy	Certification Policy

LVR G2 Root CA 01	
X.509 Version	V3
Serial Number	51 20 b8 3e 7c b1 6d 8c 44 b4 13 5c 99 8f 1a 24
Signature Algorithmus	SHA256
Aussteller	CN = LVR G2 Root CA 01 O = Landschaftsverband Rheinland C = DE
Schlüssellänge	4096
Gültig ab	12. Oktober 2016 13:41:56
Gültig bis	12. Oktober 2031 13:47:16
Öffentlicher Schlüssel	RSA (4096-Bit) Key Blob
Gegenstand	CN = LVR G2 Root CA 01 O = Landschaftsverband Rheinland C = DE
Schlüsselverwendung	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Subject Key Identifier	9d 56 aa 5f 47 85 4a 48 7f 44 25 88 2d a8 39 60 ba 43 04 35
Authority Key Identifier	None
CRL Distribution Points	None
Authority Information Access	None
Subject Alternative Name	None
Extended Key Usage	None
Thumbprint Algorithm	SHA1
Thumbprint	d9 a2 1c 16 6d 78 a2 21 13 eb d0 19 4c a6 6d 0e 41 5b 04 38
Certificate Policies	1.3.6.1.4.1.28973.509.2.20 LVR PKI G2 Certificate Policy

LVR G2 Sub CA 01	
X.509 Version	V3
Serial Number	64 00 00 00 02 13 46 9d f5 da 4b 87 8e 00 00 00 00 00 02
Signature Algorithmus	SHA256
Aussteller	CN = LVR G2 Root CA 01 O = Landschaftsverband Rheinland C = DE
Schlüssellänge	4096
Gültig ab	26. Oktober 2016 13:02:22
Gültig bis	26. Oktober 2023 13:12:22
Öffentlicher Schlüssel	RSA (4096-Bit) Key Blob
Subject	CN = LVR G2 Sub CA 02 O = Landschaftsverband Rheinland C = DE
Schlüsselverwendung	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Subject Key Identifier	70 44 9a 13 38 17 7f c2 05 eb db 8c a4 4b 4b b6 0f 4b 1b 8d
Authority Key Identifier	9d 56 aa 5f 47 85 4a 48 7f 44 25 88 2d a8 39 60 ba 43 04 35
CRL Distribution Points	http://cdp.pki.lvr.de/cdp/LVR%20G2%20Root%20CA%2001.crl
Authority Information Access	http://aia.pki.lvr.de/aia/LVR%20G2%20Root%20CA%2001.crt
Subject Alternative Name	None
Extended Key Usage	None
Thumbprint Algorithm	SHA1
Thumbprint	39 16 f3 17 f6 4d e5 a8 cb 1d 03 0e 3c 15 b7 f3 b6 05 4e 05
Certificate Policies	1.3.6.1.4.1.28973.509.2.20.10.1 LVR PKI G2 Certificate Policy

LVR G2 Sub CA 02	
X.509 Version	V3
Serial Number	64 00 00 00 03 a5 b4 6c fb 42 f9 d7 be 00 00 00 00 00 03
Signature Algorithm	SHA256
Issuer	CN = LVR G2 Root CA 01 O = Landschaftsverband Rheinland C = DE
Key Length	4096
Valid from	26. Oktober 2016 13:03:16
Valid to	26. Oktober 2023 13:13:16
Public Key	RSA (4096-Bit) Key Blob
Subject	CN = LVR G2 Sub CA 02 O = Landschaftsverband Rheinland C = DE
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Subject Key Identifier	2d a6 65 f7 77 3a 1c 08 aa 34 83 72 47 51 02 1e f9 80 f1 a0
Authority Key Identifier	9d 56 aa 5f 47 85 4a 48 7f 44 25 88 2d a8 39 60 ba 43 04 35
CRL Distribution Points	http://cdp.pki.lvr.de/cdp/LVR%20G2%20Root%20CA%2001.crl
Authority Information Access	http://aia.pki.lvr.de/aia/LVR%20G2%20Root%20CA%2001.crt
Subject Alternative Name	None
Extended Key Usage	None
Thumbprint Algorithm	SHA1
Thumbprint	6a 90 87 93 c7 3b 56 20 ea 20 dc e7 2c 39 7f 81 e4 24 ff 9e
Certificate Policies	1.3.6.1.4.1.28973.509.2.20.10.1 LVR PKI G2 Certificate Policy

9.1.1 Version Nummer(s)

Die Zertifizierungsstellen der LVR PKI G2 stellen X.509 Version 3 Zertifikate aus.

9.1.2 Zertifikats Erweiterungen

Folgende Zertifikatserweiterungen werden in den von der LVR bereitgestellten Zertifikaten berücksichtigt:

Erweiterung	Wert	Kritisch
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	Ja
Basic Constraints	Subject Type=CA Path Length Constraint= • 1 für LVR G2 Root CA 01 • 0 für LVR G2 Sub CA 01/02	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	1.3.6.1.4.1.28973.509.2.20.10.1 (LVR-InfoKom CP/CPS OID Referenz)	Nein

9.1.3 Algorithm Object Identifiers

Die Zertifizierungsinstanzen der LVR PKI G2 erstellen Signaturen mit sha256WithRSAEncryption
(OID: 1.2.840.113549.1.1.11) gemäß RFC 5280.

9.1.4 Name Forms

Die von den Zertifizierungsinstanzen der LVR PKI G2 ausgestellten CA Zertifikate enthalten den kompletten DN (Distinguished Name) im Subject Name und im Issuer Name Feld. Der Aufbau des DNs erfolgt gemäß RFC 5280 und enthält die Komponenten in folgender Reihenfolge:
DN für subject name/issuer name =

CN = [common name],

O = [organization],

C = [country]

9.1.5 Name Constraints

Nichtzutreffend. Es existieren keine Beschränkungen bezogen auf Namen.

9.1.6 Certificate Policy Object Identifier

Die LVR PKI G2 Certificate Policy OID lautet: 1.3.6.1.4.1.28973.509.2.20.

9.1.7 Policy Constraints Extension

Die Policy Constraint Extension restriktiert die Pfadlänge in der Vertrauenskette

Zertifizierungsinstanz	**Länger der Vertrauenskette**	**Parameter**
LVR G2 Root CA 01	1	Path Length = 1
LVR G2 Sub CA 01	0	Path Length = 0
LVR G2 Sub CA 02	0	Path Length = 0

9.1.8 Policy Qualifiers Syntax und Semantik

Die LVR PKI G2 Certificate Policy Qualifier ID ist:

- LVR PKI G2 OID: 1.3.6.1.4.1.28973.509.2.20.10.1

Die LVR PKI G2 CP/CPS Lokation wird durch eine URL bereitgestellt:

- http://www.pki.lvr.de/

9.1.9 Processing Semantics für kritische Certificate Policies Extension

Nichtzutreffend.

9.2 CRL Profil

CRLs werden in Rahmen der LVR PKI G2 ausgegeben. Eine Ausgabe von Delta CRLs ist für die LVR G2 Sub CA 01 und LVR G2 Sub CA 02 vorgesehen. Eine Ausgabe von Delta CRLs für die LVR G2 Root CA 01 nicht geplant. Delta CRLs werden ausschließlich im LVR Verzeichnisdienst veröffentlicht.

LVR 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

Die Basis CRL Felder sind wie folgt festgelegt:

Feld	**Wert**
Version	Siehe auch 9.2.1 *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 9.1.3 *Algorithm Object Identifiers*
Signature	CAs signature

LVR G2 Root CA 01 – CRL Profil	
Feld	**Wert**
Version	X.509 V2
Issuer	CN = LVR G2 Root CA 01 O = Landschaftsverband Rheinland C = DE
This update / Valid from	[Time and date of CRL issuance]
Next update	[Time and date of next CRL update]
Signature Algorithm	SHA256RSA
Extension	**Wert**
Authority Key Identifier	9d 56 aa 5f 47 85 4a 48 7f 44 25 88 2d a8 39 60 ba 43 04 35
CRL Number	[Unique increasing number per CRL]
CA Version	Starting from: V0.0
Next CRL Publish	[Time and date of next CRL publish]
Revoked Certificates	**Wert**
Certificate Serial Number	[Serial Number of revoked Certificate]
Revocation Date	[Time and date of Certificate revocation]
Reason Code	Revocation Reason: unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL

LVR G2 Sub CA 01 – CRL Profil	
Feld	**Wert**
Version	X.509 V2
Issuer	CN = LVR G2 Sub CA 01 O = Landschaftsverband Rheinland C = DE
This update / Valid from	[Time and date of CRL issuance]
Next update	[Time and date of next CRL update]
Signature Algorithm	SHA256RSA
Extension	**Wert**
Authority Key Identifier	70 44 9a 13 38 17 7f c2 05 eb db 8c a4 4b 4b b6 0f 4b 1b 8d
CRL Number	[Unique increasing number per CRL]
CA Version	Starting from: V0.0
Next CRL Publish	[Time and date of next CRL publish]
Revoked Certificates	**Wert**
Certificate Serial Number	[Serial Number of revoked Certificate]
Revocation Date	[Time and date of Certificate revocation]
Reason Code	Revocation Reason: unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL

LVR G2 Sub CA 02 – CRL Profil	
Feld	**Wert**
Version	X.509 V2
Issuer	CN = LVR G2 Sub CA 02 O = Landschaftsverband Rheinland C = DE
This update / Valid from	[Time and date of CRL issuance]
Next update	[Time and date of next CRL update]
Signature Algorithm	SHA256RSA
Extension	**Wert**
Authority Key Identifier	2d a6 65 f7 77 3a 1c 08 aa 34 83 72 47 51 02 1e f9 80 f1 a0
CRL Number	[Unique increasing number per CRL]
CA Version	Starting from: V0.0
Next CRL Publish	[Time and date of next CRL publish]
Revoked Certificates	**Wert**
Certificate Serial Number	[Serial Number of revoked Certificate]
Revocation Date	[Time and date of Certificate revocation]
Reason Code	Revocation Reason: unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL

9.2.1 Version Number(s)

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

9.2.2 CRL und CRL Entry Extensions

CRL Extensions (Erweiterungen) können aus dem aktuell für die LVR PKI G2 geltenden CRL Profil entnommen werden. Siehe auch *7.2. CRL Profile*.

9.3 OCSP Profil

Der OCSP Dienst ist ein Weg zur Überprüfung der Sperrinformation eines einzelnen Zertifikats. Der OCSP Dienst liefert für die LVR G2 Sub CA 01 und LVR G2 Sub CA 02 die Sperrinformation eines Zertifikats mit maximalen Latenz von 8 Stunden. Der Regelbetrieb liefert die Statusinformation mit einer maximalen Latenz von 5 Minuten.
Die Statusinformationen werden mit einem Zertifikat signiert, das von der LVR G2 Sub CA 01 ausgestellt wurde.

9.3.1 Version Number(s)

Nichtzutreffend.

9.3.2 OCSP Erweiterungen

9.3.2.1 OCSP nonce Unterstützung

Der OCSP Dienst unterstützt keinen NONCE in den OCSP anfragen.

9.3.2.2 OCSP TTL

Der OCSP Dienst verwendet die Delta CRL Sperrlisten Informationen für die Time-To-Live (TTL) in den OCSP anfragen

10 Auditierung und Überprüfung der Konformität

In Rahmen der LVR PKI G2 werden interne Audits (ISO 27001 Zertifizierung) durchgeführt, um Abweichungen vom Regelbetrieb der LVR G2 Root CA 01 zu den Ausführungen in der LVR Certificate Policy bzw. Certification Practice Statement (CP/CPS) zu identifizieren, und bei aufgedeckten Abweichungen der Konformität notwendige korrektive Maßnahmen zu ergreifen.

10.1 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 IT-Infrastruktur festgelegt. Eine Detailbeschreibung der Umstände und das Zeitschema für die Überprüfungsintervalle kann von der IT-Infrastruktur erfragt werden.

10.2 Identität und Qualifikation des Prüfers/Auditors

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

10.3 Verhältnis des Prüfers zur überprüften Entität

Der zugewiesene Auditor für die Überprüfung der Konformität ist zur überprüften Entität, nämlich der LVR PKI G2 (Technologie und Prozesse) organisatorisch unabhängig.

10.4 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

10.5 Maßnahmen bei Nichterfüllung oder Abweichen von der Konformität

Werden Abweichungen zur Konformität festgestellt so müssen diese zeitnah korrigiert werden. Hierzu wird ein Aktionsplan entwickelt, welche die notwendigen Maßnahmen beschreiben um die notwendigen Korrekturen auszuführen. Die Entwicklung und Implementierung des Aktionsplans obliegt der IT-Infrastruktur.
Nach Umsetzung des Aktionsplans gilt es zu überprüfen ob die ausgeführten Maßnahmen zu einer Korrektur der Mängel geführt haben. Das LVR-InfoKom Vorstand wird über die erzielten Ergebnisse informiert.

10.6 Kommunikation der Prüfergebnisse

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

11 Weitere rechtliche und geschäftliche Regelungen

Dieser Abschnitt bezieht sich auf die geschäftlichen-, rechtlichen- und Datenschutz-Aspekte der LVR PKI G2.

11.1 Gebühren

Nichtzutreffend.

11.1.1 Gebühren für die Ausstellung und Erneuerung von Zertifikaten

Nichtzutreffend.

11.1.2 Gebühren für den Zugriff auf Zertifikate

Nichtzutreffend.

11.1.3 Gebühren für den Zugriff auf Speerlisten- oder Status-Information

Nichtzutreffend.

11.1.4 Gebühren für weitere Dienste

Nichtzutreffend.

11.1.5 Richtlinie für die Erstattung von Gebühren

Nichtzutreffend.

11.2 Finanzielle Verantwortung

11.2.1 Versicherungsschutz

Ein Versicherungsschutz ist nicht gegeben.

11.2.2 Vermögenswerte

Vermögenswerte werden nicht abgedeckt.

11.2.3 Versicherungsschutz oder Gewährleistung für Zertifikatsnehmer

Ein Versicherungsschutz für Zertifikatnehmer ist nicht gegeben.

11.3 Vertraulichkeit von Geschäftsinformationen

11.3.1 Vertrauliche Informationen berücksichtigt

Jegliche Informationen über Teilnehmer und Antragsteller, die nicht unter 9.3.2 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.

11.3.2 Vertrauliche Informationen nicht berücksichtigt

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

11.3.3 Verantwortung zum Schutz vertraulicher Informationen

Jede innerhalb der LVR PKI G2 operierende Zertifizierungsstelle (Sub-CA) trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen.

11.4 Datenschutz (personenbezogen)

11.4.1 Datenschutzrichtlinie/-plan

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

11.4.2 Vertraulich zu behandelnde Informationen

Jegliche Informationen über Zertifikatsnehmer und Antragsteller sind vertraulich zu behandeln.

11.4.3 Nicht vertraulich zu behandelnde Informationen

Nicht vertraulich sind Informationen die in den öffentlichen Zertifikaten, wie im LVR Benutzerzertifikat oder im Zertifizierungsstellen-Zertifikat, enthalten sind. Ebenfalls gilt es für Informationen, die in den öffentlichen Zertifikatssperrlisten (CRLs) enthalten sind.

11.4.4 Verantwortung zum Schutz personenbezogener Information

Der LVR G2 Root CA 01 Betrieb ist verantwortlich für den Schutz vertraulicher Informationen. Eine Offenlegung von vertraulichen Informationen kann nur in Abstimmung mit den verantwortlichen Stellen geschehen. Näheres hierzu kann bei der IT-Infrastruktur erfragt werden.

11.4.5 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.

11.4.6 Offenlegung bei gerichtlicher Anordnung oder in Rahmen einer gerichtlichen Beweisführung

LVR-InfoKom richtet sich bei der Speicherung und Verarbeitung von personenbezogenen Daten den gesetzlichen Datenschutzbestimmungen. Eine Offenlegung findet nur gegenüber staatlichen Instanzen statt, wenn entsprechende Anordnungen ausgegeben wurden.

11.4.7 Andere Umstände einer Veröffentlichung

Keine.

11.5 Urheberrechte

Landschaftsverband Rheinland besitzt die Urheberrechte für ausgegebene Dokumentationen in Rahmen der LVR PKI G2.

11.6 Verpflichtungen

11.6.1 Verpflichtung der Zertifizierungsstellen

Zertifizierungsstellen des Landschaftsverband Rheinland verpflichten sich den aufgestellten Bestimmungen der CP bzw. CPS Dokumentation zu folgen.

11.6.2 Verpflichtung der Registrierungsstellen

Registrierungsstellen im Rahmen der LVR PKI G2 verpflichten sich den aufgestellten Bestimmungen der CP bzw. CPS Dokumentation zu folgen.

11.6.3 Verpflichtung des Zertifikatsnehmers

Die Nutzung der Zertifikate durch den Zertifikatsnehmer hat den LVR PKI G2 Zertifikatsrichtlinien zu folgen. In Kapitel 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.

11.6.4 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.

11.6.5 Verpflichtung anderer Teilnehmer

Nichtzutreffend.

11.7 Gewährleistung

Grundsätzlich wird keine Gewährleistung übernommen. Die LVR-InfoKom stellt die notwendigen IT Ressourcen für den Betrieb der LVR PKI G2 zur Verfügung, aber ohne eine garantierte Verfügbarkeit.

11.8 Haftungsbeschränkung

LVR-InfoKom übernimmt keinerlei Haftung für Sach- und Vermögensschäden. Insbesondere bei einer unsachgemäßen oder einer grob fahrlässigen Nutzung der LVR PKI G2 erlischt jegliche Haftung gegenüber Dritten.

11.9 Haftungsfreistellung

Bei der unsachgemäßen Verwendung des Zertifikats und dem zu Grunde liegenden privaten Schlüssels oder einer Verwendung des Schlüsselmaterials beruhend auf fälschlichen oder fehlerhaften Angaben bei der Beantragung, ist LVR-InfoKom von der Haftung freigestellt.

11.10 Inkrafttreten und Aufhebung

11.10.1 Inkrafttreten

Nach Veröffentlichung der aktuellen LVR CP/CPS Dokumentation tritt dies auch in Kraft. Die Veröffentlichung erfolgt auf der im Zertifikat vorgegebenen URL:

- http://cps.pki.lvr.de/cps/LVR%20G2%20CPCPS.pdf

11.10.2 Aufhebung

Dieses Dokument ist solange gültig, bis

- es durch eine neue Version ersetzt wird oder
- der Betrieb der
    - LVR G2 Root CA 01 Zertifizierungsstelle
    - LVR G2 Sub CA 01 Zertifizierungsstelle
    - LVR G2 Sub CA 02 Zertifizierungsstelle

  eingestellt wird.

11.10.3 Konsequenzen der Aufhebung

Keine.

11.11 Individuelle Benachrichtigung und Kommunikation mit Teilenehmern

Die individuelle Benachrichtigung der LVR PKI G2 Teilnehmer obliegt der IT-Infrastruktur.

11.12 Ergänzungen der Richtlinie

Die Ergänzung und Modifikation der CP bzw. CPS Dokumentation Teilnehmer obliegt der IT-Infrastruktur. In Abschnitt 1.5. sind entsprechende Kontaktdaten veröffentlicht.

11.12.1 Prozess für die Ergänzung der Richtlinie

Nichtzutreffend.

11.12.2 Benachrichtigungsmethode und -zeitraum

Nichtzutreffend.

11.12.3 Bedingungen für die Änderung einer OID

Nichtzutreffend.

11.13 Schiedsverfahren

Nichtzutreffend.

11.14 Gerichtsstand

- Die Gesellschaft LVR-InfoKom ist beim Amtsgericht Köln eingetragen – B 40276
- Umsatzsteuer-Identifikationsnummer: DE 121860628
- Gerichtsstand: Köln

Der Betrieb der LVR PKI G2 unterliegt den Gesetzen der Bundesrepublik Deutschland. Der Gerichtsstand ist Köln, Bundesrepublik Deutschland. Dieser Gerichtsstand gilt auch für Parteien deren Wohnsitz oder der gewöhnliche Aufenthaltsort ins Ausland verlegt wird oder unbekannt ist.

11.15 Konformität zum geltenden Recht

Die von der LVR PKI G2 ausgestellten Zertifikate sind nicht konform zu qualifizierten Zertifikaten. Die Vorgaben und Richtlinien nach deutschem Signaturgesetzt [SigG] sind daher nicht bindend für den Betrieb der LVR PKI G2.

12 Weitere Regelungen

12.1 Vollständigkeit

Alle in der CP & CPS für das Personen PKI beschriebenen Regelungen gelten zwischen den von der LVR-InfoKom betriebenen Zertifizierungsstellen und deren Zertifikatnehmern. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

12.2 Übertragung der Rechte

Eine Übertragung der Rechte ist nicht vorgesehen.

12.3 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 als vereinbart, welche dem Sinn und Zweck der unwirksamen Bestimmung entspricht. Im Falle von Lücken, gilt dasjenige als vereinbart, was nach Sinn und Zweck dieses Vertrages vernünftigerweise vereinbart worden wäre, hätte man die Angelegenheit von vorn herein 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.

12.4 Erzwingungsklausel

Rechtliche Auseinandersetzungen, die aus dem Betrieb einer von der LVR-InfoKom betriebenen Zertifizierungsstelle herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland.
Erfüllungsort und ausschließlicher Gerichtsstand ist Köln, Bundesrepublik Deutschland.

12.5 Höhere Gewalt

LVR-InfoKom 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.

12.6 Andere Regelung

Keine.

13 Definitionen und Abkürzungen

Abkürzung	Definition
ABA (American Bar Association)	Verband der amerikanischen Revisoren
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)	Kryptographie Standard der US Behörden
HSM (Hardware Security Module)	Hardwarekomponente, das sicherheitsrelevante Informationen wie Daten und kryptographische Schlüssel sicher speichert und verarbeitet
IETF (Internet Engineering Task Force)	Projektgruppe für die technische Weiterentwicklung des Internets. Spezifiziert quasi 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 Identifikation, 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)	Beschreibung von Technologie, Prozesse und Teilnehmer in Rahmen der asymmetrischen Kryptographie
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 Location im Internet
X.500	Protokolle und Dienste für ISO konforme Verzeichnisse
X.509	Authentifikationsmethode für X.500 Verzeichnisse
X.509v3	Aktuell gültiger PKI Zertifikatsstandard