LVR InfoKom Das Systemhaus

Qualität für Menschen

CP/CPS Landschaftsverband Rheinland

PKI G3/G4

Zertifikatsrichtlinie (CP) & Erklärung zum Zertifizierungsbetrieb (CPS)

Version:	2.0.0
Stand:	07.10.2025
Status:	Abgenommen
Erstellt von:	Gürkan Aydin
Verantwortlich:	Gürkan Aydin

Vertraulichkeitsklassifizierung: öffentlich

LVR InfoKom, Hermann-Pünder-Str. 1, D-50679 Köln

Tel.: 0221 809 7670
Mail: Guerkan.Aydin@lvr.de
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 Autorenschaft 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
1.0.4	15.01.2018	Gürkan Aydin	Jährliche Durchsicht ohne Änderungen
1.0.5	04.02.2019	Gürkan Aydin	Jährliche Durchsicht ohne Änderungen
1.0.6	16.03.2020	Gürkan Aydin	Jährliche Durchsicht
1.0.7	06.05.2021	Gürkan Aydin	Jährliche Durchsicht ohne Änderungen
1.0.9	18.06.2021	Gürkan Aydin	Adresse und Telefonnummer aktualisiert
1.1.0	30.05.2022	Gürkan Aydin	Jährliche Durchsicht
1.1.1	05.05.2023	Gürkan Aydin	jährliche Durchsicht ohne Änderung
1.1.2	22.05.2024	Gürkan Aydin	Anpassungen: - Verwendungszweck Sub CA 01 - Kontaktperson - Gültigkeit von Zertifikaten und Schlüsselpaaren
1.1.3	25.09.2025	Gürkan Aydin	Umfassende Aktualisierung
2.0.0	07.10.2025	Lutz Knüchel	QS

Abnahmehistorie

Version	Datum	Beschlossen durch	Hinweise
1.0.3	06.02.2017	Philipp Franzen	
1.0.4	18.01.2018	Philipp Franzen	
1.0.5	12.03.2019	Lutz Knüchel	
1.0.6	14.05.2020	Lutz Knüchel	
1.0.7	06.05.2021	Lutz Knüchel	
1.0.9	18.06.2021	Lutz Knüchel	
1.1.0	31.05.2022	Lutz Knüchel	
1.1.1	05.05.2023	Lutz Knüchel	
1.1.2	23.05.2024	Lutz Knüchel	
2.0.0	07.10.2025	Lutz Knüchel	

Inhaltsverzeichnis

1 Einleitung

Der Begriff Certificate Policy (CP), im X.509-Standard definiert, bezeichnet die Gesamtheit der Regeln und Vorgaben, die die Anwendbarkeit eines Zertifikatstyps bestimmen. Die Zielsetzung einer CP wird im RFC 3647 („Certificate Policy and Certification Practices Framework“) ausführlich erläutert. Eine CP dient den Nutzern eines Zertifikats als Entscheidungshilfe, ob einem bestimmten Zertifikat und dessen Verwendung vertraut werden kann.
Eine CP sollte mindestens folgende Aspekte enthalten:

- Welche technischen und organisatorischen Anforderungen die Systeme und Prozesse bei der Ausstellung der Zertifikate erfüllen müssen,

- Welche Vorgaben für die Nutzung der Zertifikate sowie für den Umgang mit den Schlüsseln und Signaturerstellungseinheiten (z. B. Chipkarten) gelten,

- Welche Bedeutung den Zertifikaten und ihren Anwendungen zukommt — also etwa welche Sicherheit, Beweiskraft oder rechtliche Relevanz die mit ihnen erzeugten Ciphertexte oder Signaturen besitzen.

Das Konzept des Certification Practice Statement (CPS) stammt von der American Bar Association (ABA) und ist in deren Digital Signature Guidelines enthalten. Eine CPS beschreibt detailliert den operativen Betrieb der Zertifizierungsstelle in einer Organisation. In der Praxis veröffentlichen Betreiber von Zertifizierungsstellen üblicherweise eine CPS. In einer unternehmensweiten PKI bietet die CPS ein Instrument zur internen Absicherung und zugleich zur transparenten Darstellung der Abläufe gegenüber Zertifikatsnehmern und vertrauenden Parteien.
Ein zentraler Zweck der CP/CPS des Landschaftsverbands Rheinland (LVR) ist die Festlegung der Vertrauenswürdigkeit der vom LVR-Rechenzentrum ausgegebenen Zertifikate und des betriebenen Zertifizierungsdienstes. Mit der Nutzung der LVR-Zertifizierungsdienste akzeptieren LVR-Mitarbeitende sowie vertrauende Parteien (z. B. in den an den IT-Verbund angeschlossenen Kliniken) die in der CP/CPS festgelegten Bedingungen und Regularien.
Die Struktur des Dokuments folgt den Empfehlungen des RFC 3647. Entsprechend legt die LVR-CP/CPS Verfahren fest, die der Zertifizierungsdienst bei Beantragung, Generierung, Auslieferung und Verwaltung der Zertifikate anwendet.
Zur Vereinfachung der Dokumentverwaltung wurden CP und CPS in einem einzigen Dokument zusammengeführt. Dieses Dokument beschreibt sowohl die Zertifikatsrichtlinie als auch die Erklärung zum Zertifizierungsbetrieb der **LVR-PKI G3/G4**. Es wird kostenfrei verteilt und ist öffentlich für LVR-Mitarbeiter zugänglich.

1.1 Überblick

LVR-InfoKom betreibt Zertifizierungsdienste für die Erzeugung, Ausgabe und Verwaltung von Zertifikaten. Die Root CAs der LVR PKI G3/G4 bilden die Vertrauensanker und ermöglichen die kontrollierte und automatisierte Ausgabe von Zertifikaten. Das nachfolgende Schaubild gibt einen Überblick über die LVR PKI G3/G4. Die Zertifizierungsinfrastruktur ist hierarchisch aufgebaut und terminiert jeweils an einer Root CA.
Neben den betriebenen CAs werden ein zentrales Zertifikatsmanagementsystem sowie Enrollment Services eingesetzt. Für das Enrollment von Server- und Clientzertifikaten stehen ausschließlich das klassische, auf DCOM basierende Verfahren sowie die CEP/CES-Services zur Verfügung. Weitergehende Informationen zu den unterstützten Enrollment Services können bei Bedarf angefordert werden. Die entsprechenden Kontaktinformationen sind in Kapitel 3.2 aufgeführt.

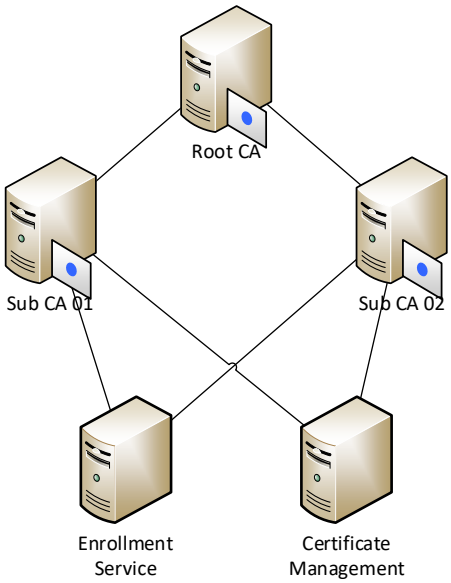

Figure 1: LVR PKI G3/G4-Umgebung

1.2 Beschreibung der Zertifikatsinstanzen

Die Aufgaben der einzelnen Zertifizierungsinstanzen werden in den folgenden Kapiteln erläutert. Detaillierte Informationen zur PKI-Architektur können bei Bedarf angefordert werden. Die entsprechenden Kontaktinformationen finden sich in Kapitel 3.2.

1.2.1 LVR G3/G4 Root CA 01

Die Zertifizierungsinstanzen LVR G3 Root CA 01 und LVR G4 Root CA 01 bilden die Vertrauensanker der LVR PKI G3/G4. Sie werden ausschließlich zur Signierung nachgeordneter Sub CAs eingesetzt. Eine direkte Ausstellung von Endentitätszertifikaten ist nicht vorgesehen.

1.2.2 LVR G3/G4 Sub CA 01

Die Zertifizierungsinstanz LVR G3 Sub CA 01 bzw. LVR G4 Sub CA 01 wird für die Ausstellung von Benutzerzertifikaten eingesetzt. Dazu gehört das folgende Zertifikatstyp:

- Authentifizierungszertifikate zur sicheren Anmeldung von Benutzern an Webdiensten.

1.2.3 LVR G3/G4 Sub CA02

Die Zertifizierungsinstanzen LVR G3 Sub CA 02 und LVR G4 Sub CA 02 werden für die Ausstellung von Maschinenzertifikaten genutzt. Dazu gehören insbesondere:

- Computerzertifikate zur Identifikation von Arbeitsplatzrechnern,
- TLS/SSL-Zertifikate zur verschlüsselten Kommunikation über unsichere Netzwerke sowie zum Schutz besonders sensibler Daten.

1.3 Dokumentation und Identifikation

Dieses Dokument stellt die Zertifikatsrichtlinie (CP) sowie die Erklärung zum Zertifizierungsbetrieb (CPS) der LVR G3/G4 Root CA des Landschaftsverbands Rheinland dar. Dem Dokument ist ein eindeutiger ASN.1 Object Identifier (OID) zugewiesen. Die LVR-OID ist bei der IANA registriert (siehe: IANA Enterprise Numbers).

Kontakt:
Landschaftsverband Rheinland (LVR)
Hermann-Pünder-Str. 1
50679 Köln
Tel.: +49 (221) 809-7670
E-Mail: Infokom.IT.Security.Services@lvr.de
Web: https://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 G3 PKI OID:** 1.3.6.1.4.1.28973.509.3
  OID Beschreibung: Namensraum der LVR PKI G3

- **LVR G4 PKI OID:** 1.3.6.1.4.1.28973.509.4
  OID Beschreibung: Namensraum der LVR PKI G4

Die CP/CPS-Dokumentationen des Landschaftsverbands Rheinland (LVR) für Zertifikatsnehmer und vertrauende Parteien sind unter folgender Adresse verfügbar:
http://www.pki.lvr.de

Die vollständigen Distinguished Names (DN) der beteiligten Zertifizierungsinstanzen lauten:

- **LVR G3 Root CA 01**
  CN = LVR G3 Root CA 01
  O = Landschaftsverband Rheinland
  C = DE

- **LVR G3 Sub CA 01**
  CN = LVR G3 Sub CA 01
  O = Landschaftsverband Rheinland
  C = DE

- **LVR G3 Sub CA 02**
  CN = LVR G3 Sub CA 02
  O = Landschaftsverband Rheinland
  C = DE

- **LVR G4 Root CA 01**
  CN = LVR G4 Root CA 01
  O = Landschaftsverband Rheinland
  C = DE

- **LVR G4 Sub CA 01**
  CN = LVR G4 Sub CA 01
  O = Landschaftsverband Rheinland
  C = DE

- **LVR G4 Sub CA 02**
  CN = LVR G4 Sub CA 02
  O = Landschaftsverband Rheinland
  C = DE

1.4 Weitere unterstützte Zertifikatsrichtlinien

Alle CAs unterstützen alle Applikationsrichtlinien.

1.5 Zertifizierungsstellen

Die LVR PKI G3/G4 besteht aus den folgenden Zertifizierungsstellen:

Zertifizierungsstelle	Laufzeit	CRL Laufzeit
LVR G3/G4 Root CA 01	15 Jahre	3 Monate + 1 Monat Überlappungszeitraum
LVR G3/G4 Sub CA 01	7 Jahre	7 Tage + 3 Tage Überlappungszeitraum
LVR G3/G4 Sub CA 02	7 Jahre	7 Tage + 3 Tage Überlappungszeitraum

1.5.1 LVR G3/G4 Root CA 01

Die Root CAs LVR G3 Root CA 01 und LVR G4 Root CA 01 basieren jeweils auf einem selbstsignierten CA-Zertifikat. Beide Root CAs sind vollständig vom Produktionsnetz getrennt und verfügen über eine dedizierte Anbindung an ein Hardware Security Module (HSM). Sie befinden sich im Offline-

Betrieb und sind zu keiner Zeit mit dem Client-Netzwerk verbunden. Sämtliche kryptographischen Operationen werden ausschließlich durch das HSM ausgeführt.

Die Root CAs stellen CA-Zertifikate sowie Sperrlisten (CRLs) für nachgeordnete Zertifizierungsstellen (Sub CAs) und für sich selbst aus.

Für die Root CAs gelten folgende Lebensdauern:

- Root-CA-Zertifikat: 15 Jahre
- Root-CA-CRLs: 3 Monate (Publikationsintervall 3 Monate, Überlappungszeitraum 1 Monat)

1.5.2 LVR G3/G4 Sub CA 01

Die Sub CAs LVR G3 Sub CA 01 und LVR G4 Sub CA 01 basieren jeweils auf einem von der entsprechenden Root CA signierten CA-Zertifikat. Beide Sub CAs sind als Online-CAs in das LVR-Netz eingebunden und werden durch Firewalls gegen unberechtigte Zugriffe geschützt.

Das private Schlüsselmaterial wird durch ein Hardware Security Module (HSM) gesichert. Die Sub CAs stellen Endentitätszertifikate sowie die dazugehörigen Sperrlisten (CRLs) aus.

Für die Sub CAs gelten folgende Lebensdauern:

- Sub-CA-Zertifikat: 7 Jahre
- CRLs: 10 Tage (Publikationsintervall 7 Tage, Überlappungszeitraum 3 Tage)

1.5.3 LVR G3/G4 Sub CA 02

Die Sub CAs LVR G3 Sub CA 02 und LVR G4 Sub CA 02 basieren jeweils auf einem von der entsprechenden Root CA signierten CA-Zertifikat. Beide Sub CAs sind als Online-CAs in das LVR-Netz eingebunden und werden durch Firewalls gegen unberechtigte Zugriffe geschützt.

Das private Schlüsselmaterial wird durch ein Hardware Security Module (HSM) gesichert. Die Sub CAs stellen Endentitätszertifikate sowie die dazugehörigen Sperrlisten (CRLs) aus.

Für die Sub CAs gelten folgende Lebensdauern:

- Sub-CA-Zertifikat: 7 Jahre
- CRLs: 10 Tage (Publikationsintervall 7 Tage, Überlappungszeitraum 3 Tage)

1.6 Registrierungsstellen

Die Aufgabe der Registrierungsstelle (RA) besteht in der Überprüfung der Identität und Authentizität von Teilnehmern und Zertifikatsinhabern. Diese Funktion wird vom LVR-InfoKom wahrgenommen.

1.6.1 Registrierungsstellen LVR G3/G4 Root CA 01

Zur Identifikation natürlicher Personen kann LVR-InfoKom beim Personalwesen anfragen.

1.6.2 Registrierungsstellen LVR G3/G4 Sub CA 01

Registrierungsstelleninstanzen im Sinne dieser Certificate Policy sind Einheiten, die Zertifikatsnehmer und Antragsteller erfassen, identifizieren und in deren Auftrag Zertifikate beantragen. Die Registrierungsstelle für die LVR G3 Sub CA 01 und LVR G4 Sub CA 01 ist über ein zentrales Zertifikatsmanagementsystem implementiert.
Hauptaufgabe ist die Bereitstellung von externen Teilnehmerzertifikaten für die Kommunikation mit vertrauenden Parteien. Die Beantragung der Zertifikate erfolgt entweder manuell gemäß den definierten RA-Prozessen oder automatisiert, sofern die Identitäten über den LVR-Verzeichnisdienst eindeutig identifiziert und autorisiert sind. Darüber hinaus können Registrierungsstellen auch durch autorisierte Identitäten in Form von Autorisierungszertifikaten (Enrollment Agents) abgebildet werden.

1.6.3 Registrierungsstellen LVR G3/G4 Sub CA 02

Die Registrierungsstelle (RA) ist für die Überprüfung der Identität und Authentizität von Teilnehmern und Zertifikatsinhabern verantwortlich. Diese Aufgabe wird von LVR-InfoKom wahrgenommen.

- Zur Identifikation natürlicher Personen nutzt LVR-InfoKom das Personalwesen sowie den etablierten LVR-Verzeichnisdienst.
- Zur Identifikation von Computern erfolgt die Prüfung über den LVR-Verzeichnisdienst.

1.7 Teilnehmer und Instanzen

Teilnehmer der LVR G3 Root CA 01 und LVR G4 Root CA 01 sind ausschließlich Sub CAs innerhalb der LVR-PKI-Infrastruktur oder Sub CAs, die auf Grundlage einer entsprechenden Vereinbarung mit dem Landschaftsverband Rheinland betrieben werden.

Teilnehmer der LVR G3 Sub CA 01/02 sowie LVR G4 Sub CA 01/02 sind ausschließlich validierte Endentitäten innerhalb der LVR-PKI-Infrastruktur. Die Validierung der Identitäten erfolgt in der Regel über den LVR-Verzeichnisdienst. Die Einbindung zusätzlicher Identitäten ist zulässig, sofern diese zuvor durch LVR-InfoKom überprüft und freigegeben wurden.

1.7.1 Zertifikatsnehmer

- Zertifikatsnehmer der LVR G3 Root CA 01 und LVR G4 Root CA 01 sind ausschließlich Sub-CA-Instanzen des Landschaftsverbands Rheinland.

- Zertifikatsnehmer der LVR G3 Sub CA 01 und LVR G4 Sub CA 01 sind ausschließlich Endentitäten des Landschaftsverbands Rheinland, die im LVR-Verzeichnisdienst geführt werden.

- Zertifikatsnehmer der LVR G3 Sub CA 02 und LVR G4 Sub CA 02 sind ausschließlich Endentitäten des Landschaftsverbands Rheinland, die entweder im LVR-Verzeichnisdienst geführt oder durch die Registrierungsstelle (RA) validiert wurden.

1.7.2 Weitere Teilnehmer

Nichtzutreffend.

2 Anwendungsbereich von Zertifikaten

Die Verantwortung für die Nutzung von Schlüsseln und Zertifikaten liegt sowohl beim Zertifikatsnehmer als auch bei der vertrauenden Partei.

2.1 Zulässige Anwendung von Zertifikaten

2.1.1 Zulässige Anwendung von Zertifikaten für LVR G3/G4 Root CA 01

Die von den LVR G3 Root CA 01 und LVR G4 Root CA 01 ausgestellten Zertifikate dürfen ausschließlich für Sub-CAs innerhalb der LVR-PKI verwendet werden. Zertifikate, die im Rahmen dieser CP/CPS ausgestellt werden, können vom Zertifikatsnehmer für delegierte Funktionen einer Sub-CA genutzt werden.

2.1.2 Zulässige Anwendung von Zertifikaten für LVR G3/G4 Sub CA 01

Die von den LVR G3 Sub CA 01 und LVR G4 Sub CA 01 ausgestellten Zertifikate dürfen verwendet werden für:

- die Identifikation von Computern,
- die Identifikation von Netzwerk-infrastruktur-komponenten (z. B. Router, Firewalls, Switches),
- die Identifikation von mobilen Endgeräten,
- die Verschlüsselung und Authentifizierung der Kommunikation in unsicheren Umgebungen (VPN/IPsec),
- die verschlüsselte Kommunikation zum Schutz besonders sensibler Daten (TLS).

2.1.3 Zulässige Anwendung von Zertifikaten für LVR G3/G4 Sub CA 02

Die von den LVR G3 Sub CA 02 und LVR G4 Sub CA 02 ausgestellten Zertifikate dürfen verwendet werden für:

- die Benutzer-authentifizierung im LVR-Verzeichnisdienst,
- die Benutzer-authentifizierung in durch den LVR validierten Applikationen.

2.2 Unzulässige Anwendung von Zertifikaten

Die Nutzung der Zertifikate ist innerhalb der LVR PKI G3/G4 beschränkt und ausschließlich auf die in den vorgegebenen Anwendungsbereichen zulässigen Zwecke begrenzt. Eine Verwendung der Zertifikate für private Zwecke oder für andere Anwendungen, die von Kapitel 2 „Zulässige Anwendungen von Zertifikaten“ abweichen, ist untersagt.
Jegliche weitergehende Nutzung der Zertifikate ist unzulässig. Insbesondere ist die Zertifizierung zusätzlicher, untergeordneter Zertifizierungsstellen ausschließlich der LVR PKI G3/G4 vorbehalten. Im Sinne der Konformität mit der LVR CP/CPS sind Änderungen oder Erweiterungen der Zertifikatsnutzung unverzüglich der Administration der LVR PKI G3/G4 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
Hermann-Pünder-Str. 1
50679 Köln
Deutschland

3.2 Kontaktpersonen

Folgende Personen sind Ansprechpartner für die Verwaltung der Zertifikatsrichtlinie und der Erklärung des Zertifizierungsbetriebs der LVR PKI G3/G4:

Team IT Security
IT-Infrastruktur
LVR-InfoKom
Hermann-Pünder-Str. 1
50679 Köln
Deutschland
Tel.: +49 (221) 809-7670
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 veröffentlicht die Zertifikate der LVR G3 Root CA 01 und LVR G4 Root CA 01 über den zentralen Verzeichnisdienst. Öffentliche Informationen – wie Root-CA-Zertifikate, CRLs sowie die CP/CPS-Dokumentation – werden zusätzlich über den webbasierten Informationsdienst https://www.pki.lvr.de bereitgestellt.

4.2 Publikation von Zertifizierungsinformationen

Die Veröffentlichung der Zertifikate der LVR PKI G3/G4 erfolgt automatisiert über den LVR-Verzeichnisdienst. Eine Benutzerinteraktion ist hierfür nicht erforderlich. Vorgesehen sind folgende Veröffentlichungsorte:

Zweck	URL
LVR PKI CP und CPS	http://cps.pki.lvr.de/cps/LVR%20CPCPS.pdf
LVR PKI G3 Root CA 01 Zertifikat	http://aia-g3.pki.lvr.de/aia/LVR%20G3%20Root%20CA%2001.crt
LVR PKI G3 Root CA 01 Sperrlisten	http://cdp-g3.pki.lvr.de/cdp/LVR%20G3%20Root%20CA%2001.crl
LVR PKI G3 Sub CA 01 Zertifikat	http://aia-g3.pki.lvr.de/aia/LVR%20G3%20Sub%20CA%2001.crt
LVR PKI G3 Sub CA 01 Sperrlisten	http://cdp-g3.pki.lvr.de/cdp/LVR%20G3%20Sub%20CA%2001.crl
LVR PKI G3 Sub CA 02 Zertifikat	http://aia-g3.pki.lvr.de/aia/LVR%20G3%20Sub%20CA%2002.crt
LVR PKI G3 Sub CA 02 Sperrlisten	http://cdp-g3.pki.lvr.de/cdp/LVR%20G3%20Sub%20CA%2002.crl
LVR PKI G3 Sub CA 01/02 Online Responder	http://ocsp-g3.pki.lvr.de/ocsp
LVR PKI G4 Root CA 01 Zertifikat	http://aia.pki.lvr.de/aia/LVR%20G4%20Root%20CA%2001.crt
LVR PKI G4 Root CA 01 Sperrlisten	http://cdp.pki.lvr.de/cdp/LVR%20G4%20Root%20CA%2001.crl
LVR PKI G4 Sub CA 01 Zertifikat	http://aia.pki.lvr.de/aia/LVR%20G4%20Sub%20CA%2001.crt
LVR PKI G4 Sub CA 01 Sperrlisten	http://cdp.pki.lvr.de/cdp/LVR%20G4%20Sub%20CA%2001.crl
LVR PKI G4 Sub CA 02 Zertifikat	http://aia.pki.lvr.de/aia/LVR%20G4%20Sub%20CA%2002.crt
LVR PKI G4 Sub CA 02 Sperrlisten	http://cdp.pki.lvr.de/cdp/LVR%20G4%20Sub%20CA%2002.crl
LVR PKI G4 Sub CA 01/02 Online Responder	http://ocsp.pki.lvr.de/ocsp

Tabelle 1: Veröffentlichungsorte

4.3 Veröffentlichungsintervall

Die Veröffentlichung der Zertifikatsrichtlinie (CP) und der Erklärung zum Zertifikatsbetrieb (CPS) der LVR PKI G3/G4 erfolgt jeweils nach Erstellung oder Aktualisierung.
Die Veröffentlichung der CA-Zertifikate der LVR PKI G3/G4 erfolgt einmalig nach der Installation der jeweiligen Zertifizierungsstellen. Eine erneute Publikation findet ausschließlich bei Ablauf oder Erneuerung der CA-Zertifikate statt.
Sperrlisten (CRLs) werden gemäß dem festgelegten Publikationsintervall erstellt und unmittelbar sowohl über die PKI-Webdienste als auch im LVR-Verzeichnisdienst veröffentlicht.

4.4 Zugang zu den Informationsdiensten

Der Zugriff auf die CA-Zertifikate, Sperrlisten sowie die CP/CPS-Dokumentation der LVR PKI G3/G4 ist uneingeschränkt und damit öffentlich möglich. Vgl. hierzu auch Abschnitt 4.2 „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:

Attribut	Wert
LVR G3 Root CA 01	
Common Name (CN)	LVR G3 Root CA 01
Organization	Landschaftsverband Rheinland
Country	DE
LVR G3 Sub CA 01	
Common Name (CN)	LVR G3 Sub CA 01
Organization	Landschaftsverband Rheinland
Country	DE
LVR G3 Sub CA 02	
Common Name (CN)	LVR G3 Sub CA 02
Organization	Landschaftsverband Rheinland
Country	DE
LVR G4 Root CA 01	
Common Name (CN)	LVR G4 Root CA 01
Organization	Landschaftsverband Rheinland
Country	DE

LVR G4 Sub CA 01	
Common Name (CN)	LVR G4 Sub CA 01
Organization	Landschaftsverband Rheinland
Country	DE
LVR G4 Sub CA 02	
Common Name (CN)	LVR G4 Sub CA 02
Organization	Landschaftsverband Rheinland
Country	DE

5.1.2 Anforderung an die Bedeutung von Namen

Der Distinguished Name (DN) muss den Zertifikatnehmer eindeutig identifizieren. Reicht der DN hierfür nicht aus, kann zur Sicherstellung der Eindeutigkeit zusätzlich der Subject Alternative Name (SAN) verwendet werden. Für die Namensvergabe gelten folgende Regelungen:

- Zertifikate dürfen ausschließlich auf zulässige Namen des Zertifikatnehmers ausgestellt werden.
- Der DN der Zertifizierungsstellen der LVR PKI G3/G4 wird aus den Namensobjekten Common Name (CN), Organisation (O) und Country (C) gebildet. Mit diesen Attributen ist die Eindeutigkeit sicherzustellen.
- Der DN der Sub-CAs wird ebenfalls aus den Namensobjekten Common Name (CN), Organisation (O) und Country (C) gebildet. Auch hier ist die Eindeutigkeit durch diese Attribute zu gewährleisten. Die Verwendung zusätzlicher Attribute wie Organizational Unit (OU), Locality (L) oder State (ST) ist zulässig, jedoch optional.

5.1.3 Anonymität und Pseudoanonymität von Zertifikatsnehmern

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

5.1.4 Regeln zur Interpretation verschiedener Namensformen

Die im Zertifikatsprofil ausgewiesenen Distinguished Names entsprechen dem X.500-Standard. E-Mail-Adressen und UPN-Einträge folgen den Vorgaben des RFC 5322 (Nachfolger von RFC 822). UPN-Namensinformationen sind in UTF-8 zu codieren.

5.1.5 Eindeutigkeit von Namen

Der vollständige Distinguished Name (DN) in den von den LVR PKI G3/G4-Zertifizierungsstellen ausgestellten Zertifikaten gewährleistet die Eindeutigkeit der Zertifikatnehmer. Zusätzlich tragen eindeutige Angaben im alternativen Namensfeld – wie die LVR-E-Mail-Adresse, der UPN-Name oder der DNS-Name von Maschinen – sowie eine eindeutige Seriennummer im Zertifikat zur Sicherstellung der Eindeutigkeit bei.
Die Verwendung eines Wildcards ist zu begründen und genehmigungspflichtig.

5.1.6 Erkennung, Authentifikation und Rolle von Warenzeichen

In der Regel ist der Distinguished Name (DN) einer Sub-CA auf technische Attribute beschränkt und besitzt daher keine Relevanz für die Anerkennung von Warenzeichen. Unabhängig davon sind sowohl die Zertifikatsnehmer als auch der Betreiber der Zertifizierungsstellen verpflichtet sicherzustellen, dass durch die automatisierte Ausstellung von Endentitätszertifikaten keine Schutzrechte an Warenzeichen verletzt werden. Die Verantwortung für die Vermeidung und Klärung möglicher Namenskonflikte liegt dabei ausschließlich beim Zertifikatsnehmer.

5.2 Identitätsprüfung bei Neuantrag

5.2.1 Verfahren zur Überprüfung des Besitzes von privaten Schlüsseln

Die Schlüsselpaare der Zertifizierungsstellen der LVR PKI G3/G4 werden durch ein Hardware Security Module (HSM) generiert. Der Besitznachweis für die privaten Schlüssel erfolgt jeweils durch die Signierung eines PKCS#10-Zertifikatsantrags (Certificate Signing Request, CSR) mit dem privaten Schlüssel. Der CSR bildet die Grundlage zur Überprüfung des Besitzes des privaten Schlüssels.
Zertifikatsnehmer der LVR G3 Root CA 01 und LVR G4 Root CA 01 sind verpflichtet, privates Schlüsselmaterial ausschließlich durch ein HSM zu schützen, sofern die CA im Online-Betrieb betrieben wird.
Zertifikatsnehmer der LVR G3 Sub CA 01/02 sowie LVR G4 Sub CA 01/02 sind verpflichtet, ihr privates Schlüsselmaterial angemessen zu sichern. Die Speicherung in Software ist zulässig, sofern sie im Einklang mit der vorgesehenen Zertifikatsnutzung steht. Eine Überprüfung des privaten Schlüsselspeichers durch die Sub CAs (Key Attestation) ist nicht vorgesehen. Mit der Teilnahme an der LVR PKI G3/G4 garantiert der Zertifikatsnehmer den ordnungsgemäßen Schutz seiner privaten Schlüssel.

5.2.2 Authentifikation der Organisation

Nichtzutreffend.

5.2.3 Authentifikation von Zertifikatsnehmern

Die Authentifizierung von Zertifikatsnehmern der LVR PKI G3/G4 erfolgt entweder über das Personalwesen des Landschaftsverbands Rheinland oder über den LVR-Verzeichnisdienst, der im Rahmen der LVR PKI als voll vertrauenswürdig eingestuft ist.

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 Benutzeridentität 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

Ein Zertifikatsrückruf erfolgt ausschließlich nach erfolgreicher Autorisierung oder im Rahmen des LVR-Incident-Managements. Die Verfahren zur Identifikation und Authentifizierung beim Zertifikatsrückruf sind im Antragswesen definiert und dokumentiert. Grundsätzlich können Zertifikatsnehmer der LVR PKI G3/G4 ihre eigenen Zertifikate widerrufen.

6 Betriebliche Anforderungen an den Zertifikatslebenszyklus

In der LVR PKI G3/G4 können Teilnehmer gemäß Abschnitt 1.7 Zertifikate beantragen. Hierfür muss für ein Zertifikat eine Autorisierung vorliegen.

6.1 Zertifikatsantrag

Im vorangegangenen Abschnitt 5~~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 G3/G4 Root CA 01	Betreiber von autorisierten LVR Sub CAs
LVR G3/G4 Sub CA 01	Aktive Benutzer aus dem LVR Verzeichnisdienst.
LVR G3/G4 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 G3/G4 Root CA 01

Der Zertifikatsnehmer informiert die RA oder die Administration der LVR G3 Root CA 01 bzw. LVR G4 Root CA 01 per E-Mail über einen Zertifikatsantrag. Dem Antrag ist die zugehörige Certificate Policy (CP) der betreffenden Sub-CA beizufügen.

6.2.2 Prozess für die Antragsbearbeitung für die LVR G3/G4 Sub CA 01 und LVR G3/G4 Sub CA 02

Der Zertifikatsnehmer übermittelt seinen Zertifikatsantrag elektronisch an das Zertifikatsmanagementsystem. Mit der Übertragung bestätigt der Antragsteller die Konformität seines Antrags mit der Zertifikatsrichtlinie der LVR PKI G3/G4.

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 Grundlage der im LVR-Verzeichnisdienst geführten Informationen zu aktiven Benutzern bzw. Antragstellern.
Die Ablehnung eines Zertifikatsantrags kann sowohl durch das Zertifikatsmanagementsystem als auch durch die LVR G3 Sub CA 01/02 bzw. LVR G4 Sub CA 01/02 erfolgen. Eine Ablehnung kann automatisiert auf Basis der Informationen im LVR-Verzeichnisdienst oder manuell durch die zuständigen Instanzen erfolgen.
Es ist zulässig, dass ein durch das Zertifikatsmanagementsystem angenommener Antrag nachträglich durch einen Zertifikatsmanager abgelehnt wird. Automatisierte Annahmen oder Ablehnungen von Zertifikatsanträgen müssen von den Zertifizierungsstellen nicht kommentiert werden.
Antragsteller können Informationen zu einem abgelehnten Zertifikatsantrag bei der zuständigen Registrierungsstelle schriftlich anfordern. Jeder Zertifikatsantrag wird mit einer eindeutigen Antragsnummer (Request-ID) versehen.

6.2.5 Verfahren zur Annahme von Zertifikatsanträge der Sub Cas

Die LVR G3 Sub CA 01/02 sowie die LVR G4 Sub CA 01/02 unterstützen verschiedene Verfahren zur Annahme von Zertifikatsanträgen.

6.2.6 Manuelle Zertifikatsanträge

Manuelle Zertifikatsanträge sind in Form einer PKCS#10-Datei per E-Mail an die Registrierungsstelle zu übermitteln. Der Antrag muss eine Begründung enthalten, warum kein automatisierter Antrag über das Zertifikatsmanagementsystem gestellt werden konnte (z. B. weil die Identität nicht im LVR-Verzeichnisdienst vorhanden ist).
Zertifikatsinformationen, die nicht durch den LVR-Verzeichnisdienst validiert werden können, sind der Registrierungsstelle plausibel darzulegen. Im Zweifelsfall ist die Registrierungsstelle berechtigt, vom Antragsteller zusätzliche Autorisierungen einzufordern.

6.2.7 Webbasierte Zertifikatsanträge

Webbasierte Zertifikatsanträge können über das Zertifikatsmanagementsystem gestellt werden. Der Zugang zu diesem System ist beim Betrieb der LVR PKI G3/G4 zu beantragen.

6.2.8 Automatisierte Zertifikatsanträge

Zertifikatsanträge an die LVR G3 Sub CA 01/02 oder LVR G4 Sub CA 01/02 sind nur zulässig, wenn sämtliche Identitäten (Subject und Subject Alternative Name) eindeutig aus den im LVR-Verzeichnisdienst geführten Informationen abgeleitet werden können.

6.2.9 HTTP-basierte Anträge

HTTP-basierte Zertifikatsanträge können über Zertifikats-Proxy-Dienste an die LVR G3 Sub CA 01/02 oder LVR G4 Sub CA 01/02 übermittelt werden. Für HTTP-basierte Anträge gelten die gleichen Bedingungen wie in Abschnitt 6.2.8 beschrieben.

6.2.10 Bearbeitungsdauer von Zertifikatsanträgen

Die Bearbeitungsdauer von Zertifikatsanträgen richtet sich nach dem jeweiligen Anwendungsfall. Manuelle Anträge werden ausschließlich während der regulären Bürozeiten des LVR-InfoKom bearbeitet. Automatisierte Anträge, deren Validierung über den LVR-Verzeichnisdienst erfolgt, werden in der Regel zeitnah verarbeitet. Verbindliche Angaben zu den garantierten Bearbeitungszeiten in den einzelnen Anwendungsfällen können beim Betrieb der LVR PKI G3/G4 erfragt werden.

6.3 Zertifikatsausgabe

Die Zertifikatsausgabe der LVR G3 Root CA 01 und LVR G4 Root CA 01 erfolgt per E-Mail oder über einen gesicherten Dateitransfer an den Antragsteller.
Die Zertifikatsausgabe der LVR G3 Sub CA 01/02 sowie LVR G4 Sub CA 01/02 erfolgt über das Zertifikatsmanagementsystem oder direkt durch die Zertifizierungsstelle anhand der im Kapitel 6.2 genannten Antragsnummer. Voraussetzung für die Zertifikatsausgabe ist eine erfolgreiche 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 jeweilige CA in angemessener Weise überprüft. Die LVR G3 Root CA 01 und LVR G4 Root CA 01 prüfen insbesondere die Berechtigung des Teilnehmers für den im Distinguished Name (DN) angegebenen Namen sowie die Gültigkeit der Signatur des Zertifikatsantrags.
Zertifikate, die von den LVR G3 Sub CA 01/02 bzw. LVR G4 Sub CA 01/02 ausgestellt werden, stehen über das Zertifikatsmanagementsystem zur Verfügung. Eine ausdrückliche Annahme durch den Antragsteller ist weder erforderlich noch vorgesehen. Zertifikate, die durch die genannten Sub CAs signiert wurden, gelten mit der Ausstellung als gültig.

6.4.2 Publikation des Zertifikats

End-Entitäten Zertifikate werden nicht 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

Im Rahmen der LVR PKI G3/G4 erfolgt eine Zertifikatserneuerung ausschließlich in Verbindung mit einem Schlüsseltausch. Eine Erneuerung mit demselben Schlüsselpaar – also ohne Schlüsselwechsel – ist nicht zulässig. Daher finden alle nachfolgenden Punkte unter Abschnitt 6.5 auf die Zertifizierungsstellen LVR G3 Root CA 01 und LVR G4 Root CA 01 keine Anwendung.

6.5.1 Umstände für eine Zertifikatserneuerung

Die Erneuerung von Zertifikaten erfolgt nach den in Kapitel 6.1 beschriebenen Voraussetzungen.

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

Im Rahmen der LVR PKI G3/G4 erfolgt die Zertifikatserneuerung ausschließlich in Verbindung mit einem Schlüsseltausch. Technisch bedeutet dies die Ersetzung eines bestehenden Zertifikats durch ein neues Zertifikat mit verlängerter Gültigkeitsdauer und einem neuen Schlüsselpaar, bei ansonsten unveränderten Zertifikatsinhalten.

6.6.1 Umstände für eine Zertifikatserneuerung mit Schlüsselwechsel

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

- die Hälfte der Gültigkeitsdauer des aktuellen Zertifikats ist abgelaufen oder steht kurz vor Ablauf,
- die im Zertifikat enthaltenen Daten sind fehlerhaft,
- der bisherige Schlüssel kann oder darf nicht mehr verwendet werden, da er (möglicherweise) kompromittiert wurde,
- die verbleibende Gültigkeitsdauer des Zertifikats oder die Schlüssellänge entspricht nicht mehr den aktuellen Sicherheitsanforderungen.

6.6.2 Antragsberechtigte für eine Zertifikatserneuerung mit Schlüsselwechsel

Antragsberechtigt für eine Zertifikatserneuerung mit Schlüsselwechsel sind alle Zertifikatsnehmer, denen von der LVR PKI G3/G4 ein gültiges Zertifikat ausgestellt 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

Im Rahmen der LVR PKI G3/G4 erfolgt die Zertifikatserneuerung ausschließlich in Verbindung mit einem Schlüsseltausch. Eine Anpassung der Zertifikatsinhalte (Datenänderung) ist nicht zulässig und wird ausschließlich über eine Neubeantragung durchgeführt. Daher finden alle nachfolgenden Punkte unter Abschnitt 6.7 auf die LVR PKI G3/G4 keine Anwendung.

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 Sperrung eines Zertifikats erfolgt auf Grundlage eines schriftlichen Antrags, der an isd@lvr.de zu richten ist. Für den Antrag wird ein Ticket erzeugt und an die zuständige Registrierungsstelle weitergeleitet. Eine sofortige Sperrung kann ausschließlich durch den LVR-Sicherheitsbeauftragten oder dessen Stellvertreter angeordnet werden. Die Durchführung der Sperrung obliegt grundsätzlich der 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

Für die Veröffentlichung von Sperrlisten (CRLs) gelten folgende Zeiträume:

- LVR G3 Root CA 01 / LVR G4 Root CA 01
  - Ausstellungszeitraum einer CRL: 4 Monate
  - Standard-Überlappungszeitraum: 1 Monat
- LVR G3 Sub CA 01/02 und LVR G4 Sub CA 01/02
  - LDAP-Veröffentlichungspfad:
    - Basis-CRL: 10 Tage (7 Tage Veröffentlichungszeitraum + 3 Tage Überlappung)
    - Delta-CRL: 6 Stunden (4 Stunden Veröffentlichungszeitraum + 2 Stunden Überlappung)
  - HTTP-Veröffentlichungspfad:
    - Basis-CRL: 10 Tage (7 Tage Veröffentlichungszeitraum + 3 Tage Überlappung)
    - Delta-CRL: 6 Stunden (4 Stunden Veröffentlichungszeitraum + 2 Stunden Überlappung)

Hinweise:

- Der LDAP-Veröffentlichungspfad wird in ausgegebenen Zertifikaten nicht referenziert und ist extern nicht erreichbar.
- Delta-CRLs dienen ausschließlich technischen Zwecken und werden weder in Basis-CRLs noch in Zertifikaten 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 G3 Root CA 01 und LVR G4 Root CA 01 unterstützen keine Online-Sperrlisten. Die LVR G3 Sub CA 01/02 sowie die LVR G4 Sub CA 01/02 stellen Online-Sperrinformationen über das Online Certificate Status Protocol (OCSP) gemäß RFC 6960 bereit.
Das für die Signatur von OCSP-Antworten verwendete Zertifikat entspricht den Vorgaben von RFC 6960. Es enthält keine eigenen Sperrinformationen; die Nichtverwendung wird über die Zertifikatserweiterung id-kp-OCSPSigning (OID 1.3.6.1.5.5.7.3.9) kenntlich gemacht.
Die Nutzung von OCSP zur Überprüfung des Sperrstatus liegt in der Verantwortung des Zertifikatsnehmers bzw. des prüfenden Systems.

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 den LVR G3 Sub CA 01/02 sowie LVR G4 Sub CA 01/02 ausgestellten Zertifikate enthalten die erforderlichen Informationen zu den zuständigen Online-Sperrservern (OCSP).

6.8.13 Weitere Arten zur Bekanntmachung von Zertifikatsstatus

Weitere Verfahren zur Bekanntmachung des Zertifikatsstatus sind nicht vorgesehen. Sperrlisten werden über Webserver und den Verzeichnisdienst veröffentlicht. Die Veröffentlichung über Webserver erfolgt über die in den Zertifikaten enthaltenen CDP-Einträge.

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 nicht vorgesehen.

6.8.16 Berechtigte für eine Suspendierung

Nichtzutreffend.

6.8.17 Durchführung einer Suspendierung

Nichtzutreffend.

6.8.18 Dauer einer Suspendierung

Nichtzutreffend.

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 Webservern der LVR PKI und verwendet HTTP als Übertragungsprotokoll. Unter der Adresse http://www.pki.lvr.de können die CRLs der Zertifizierungsstellen der LVR PKI G3/G4 über die in Kapitel 4.2 angegebenen Pfade abgerufen werden.
CRLs und die darin aufgeführten zu sperrenden Zertifikate müssen von der jeweiligen Zertifizierungsstelle der LVR PKI G3/G4 ausgestellt worden sein. Eine Unterstützung indirekter CRLs ist nicht vorgesehen. Die ausgegebenen CRLs entsprechen dem X.509 Version 2 Standard und sind vollständig konform zu RFC 5280.

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 bzw. Zertifikatsnehmer eines LVR PKI G3/G4-Zertifikats scheidet aus den Zertifizierungsdiensten aus, sobald das Zertifikat nicht mehr benötigt wird oder eine Kompromittierung 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 Zertifizierungsstellen der LVR PKI G3/G4 sind in den Rechenzentrumsbetrieb der LVR-InfoKom integriert. Die Zertifizierungsstellen werden als virtuelle Maschinen auf Hypervisoren betrieben, die den Sicherheitsvorgaben der LVR-InfoKom entsprechen. Folgende Vorkehrungen und physischen Schutzmaßnahmen sind fester Bestandteil der durch die LVR-InfoKom betriebenen Rechenzentren.

7.1.1 Lage und Konstruktion

Die Hypervisoren für den Betrieb der Zertifizierungsstellen der LVR PKI G3/G4 befinden sich in den Rechenzentrumsräumen des LVR. Diese Räume sind mit physischen Sicherheitsmaßnahmen ausgestattet, die ein dem erforderlichen Sicherheitsniveau entsprechendes Schutzniveau gewährleisten.

7.1.2 Zutrittskontrolle

Die Betriebsräume der Zertifizierungsstellen sind durch geeignete technische und infrastrukturelle Maßnahmen geschützt. Zutritt erhalten ausschließlich Mitarbeiter mit entsprechender Freigabestufe. Der Zugang betriebsfremder Personen ist nur im Rahmen der geltenden Besucherregelung zulässig.

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
- 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 vorhandener Aktenvernichter 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 im Betrieb der LVR PKI G3/G4 sind in Rollen gebündelt. Ein Rollenkonzept liegt vor und wird sowohl für organisatorische Prozesse als auch für den Betrieb der Hardware Security Module (HSM) angewendet.
Für den Betrieb der LVR G3 Sub CA 01/02 und LVR G4 Sub CA 01/02 sind folgende Rollen vorgesehen:

- CA-Administration
  - Verwaltung der CA-Server
  - Verwaltung des CA-Dienstes
  - Verwaltung der CA-Konfiguration
  - Sicherungs- und Wiederherstellungsmanagement der CA
- HSM-Administration
  - Verwaltung der HSM
  - Sicherungs- und Wiederherstellungsmanagement der HSM
- Zertifikatsadministration
  - Bearbeitung von Zertifikatsanträgen
  - Bearbeitung von Sperranträgen

Eine detaillierte Beschreibung der Rollen und ihrer Aufgaben kann bei Bedarf bei der IT-Infrastruktur angefordert 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 von Benutzern erfolgt beim Zutritt zu sicherheitsrelevanten Räumen sowie beim Zugriff auf sicherheitsrelevante Systeme durch den Einsatz von Smartcards, Hardware-Tokens und/oder Benutzername-Passwort-Kombinationen.

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

Für den Betrieb der LVR PKI G3/G4 stellt LVR-InfoKom qualifiziertes und erfahrenes Personal bereit. Die erforderlichen Qualifikationen, Kenntnisse und Erfahrungen sind vorhanden, um einen sicheren und ordnungsgemäßen PKI-Regelbetrieb zu gewährleisten.

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 Häufigkeit der Schulungen richtet sich nach den Anforderungen der LVR PKI G3/G4. Schulungen finden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme oder Sicherheitstechnologien statt.

7.3.5 Frequenz und Abfolge von Jobrotation

Eine Jobrotation 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 Betriebspersonal der LVR PKI G3/G4 ist zur Einhaltung aller relevanten Anweisungen und gesetzlichen Vorschriften verpflichtet. Dazu gehört insbesondere die Pflicht, personenbezogene Daten vertraulich zu behandeln.

7.3.8 An das Personal ausgehändigte Dokumente

Für den ordnungsgemäßen Betrieb der LVR PKI G3/G4 stehen dem LVR-Personal folgende Dokumente zur Verfügung:

- Zertifikatsrichtlinie (Certificate Policy, CP)
- Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS)
- Betriebs- und Sicherheitskonzept der Zertifizierungsinstanzen der LVR PKI G3/G4
- Handlungsanweisungen
- Betriebshandbücher der eingesetzten 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 der LVR G3 Root CA 01 und LVR G4 Root CA 01 werden gemeinsam mit anderen relevanten Daten regelmäßig gesichert.

7.4.6 Audit Collection System (Protokollierungssystem intern oder extern)

Nichtzutreffend.

7.4.7 Benachrichtigung bei Auslösen eines sicherheitskritischen Ereignisses

Nichtzutreffend.

7.5 Erfassung von Protokolldaten

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

7.5.1 Erfasste 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

Nichtzutreffend.

7.5.3 Schutzmaßnahmen für das Archiv

Nichtzutreffend.

7.6 Schlüsselwechsel der Zertifizierungsstellen

Bei einem Schlüsselwechsel der Zertifizierungsinstanzen der LVR PKI G3/G4 wird das bestehende CA-Zertifikat durch ein neues Zertifikat ersetzt. Im Fall der LVR G3 Root CA 01 und LVR G4 Root CA 01 handelt es sich dabei um ein selbstsigniertes Zertifikat, das veröffentlicht wird. Eine Sperrung eines selbstsignierten Root-CA-Zertifikats ist technisch auf CA-Seite nicht möglich. Für die LVR G3 Sub CA 01/02 sowie LVR G4 Sub CA 01/02 erfolgt eine Sperrung des Zertifikats ausschließlich im Falle einer Kompromittierung. Ein geplanter Schlüsselwechsel ist für jede CA nach der Hälfte der Zertifikatslaufzeit vorgesehen.

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 Server-/Clientzertifikate werden Zertifikate mit neuem Schlüsselmaterial ausgegeben.
- 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 G3/G4 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. Für jeglichen Prozess, der den Zugriff auf den privaten Schlüssel der Zertifizierungsstelle erforderlich macht, ist das HSM zwingend eingebunden.

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:

Zertifizierungsinstanz	Veröffentlichungspfad
LVR G3 Root CA 01	http://aia-g3.pki.lvr.de/aia/LVR%20G3%20Root%20CA%2001.crt
LVR G3 Sub CA 01	http://aia-g3.pki.lvr.de/aia/LVR%20G3%20Sub%20CA%2001.crt
LVR G3 Sub CA 02	http://aia-g3.pki.lvr.de/aia/LVR%20G3%20Sub%20CA%2002.crt
LVR G4 Root CA 01	http://aia.pki.lvr.de/aia/LVR%20G4%20Root%20CA%2001.crt
LVR G4 Sub CA 01	http://aia.pki.lvr.de/aia/LVR%20G4%20Sub%20CA%2001.crt
LVR G4 Sub CA 02	http://aia.pki.lvr.de/aia/LVR%20G4%20Sub%20CA%2002.crt

8.1.5 Schlüssellängen

Detailinformationen sind dem aktuellen LVR RFC 5280 Zertifikatsprofiltabelle zu entnehmen

CA	Schlüssellänge	Algorithmus
LVR G3 Root CA 01	4096 Bit (HSM)	RSA
LVR G3 Sub CA 01	4096 Bit (HSM)	RSA
LVR G3 Sub CA 02	4096 Bit (HSM)	RSA
LVR G4 Root CA 01	4096 Bit (HSM)	RSA
LVR G4 Sub CA 01	4096 Bit (HSM)	RSA
LVR G4 Sub CA 02	4096 Bit (HSM)	RSA

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 G3/G4 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.

8.1.11 Hinterlegung von privaten Schlüsseln

Nichtzutreffend.

8.1.12 Backup von privaten Schlüsseln

Privates Schlüsselmaterial der LVR PKI G3/G4 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 G3/G4 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 G3/G4 Root CA 01	7 Jahre
LVR G3/G4 Sub CA 01	1 Jahr
LVR G3/G4 Sub CA 02	1 Jahr

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 Malware 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 G3/G4 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 G3/G4 muss den Vorgaben der LVR-InfoKom entsprechen. Das Betriebssystem der Zertifizierungsinstanzen der LVR PKI G3/G4 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 G3/G4 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 G3/G4 Lösung nicht vorgesehen.

9 Zertifikats- und CRL Profil

In Rahmen der X.509 PKI sind Zertifikats- und CRL Profile für die LVR G3/G4 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 G3/G4 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 0*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 G3 Root CA 01	
X.509 Version	V3
Serial Number	2cc12618cc33391c1db7c03826af62c4
Signature Algorithmus	sha256RSA
Signature Hash Algorithmus	sha256
Aussteller	CN = LVR G3 Root CA 01 O = Landschaftsverband Rheinland C = DE
Schlüssellänge	4096
Gültig ab	30. Oktober 2023 11:40:14
Gültig bis	31. Oktober 2038 01:59:59
Öffentlicher Schlüssel	RSA (4096 Bits)
Antragsteller	CN = LVR G3 Root CA 01 O = Landschaftsverband Rheinland C = DE
Schlüsselverwendung	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Subject Key Identifier	95ae0e5d5210030b3bdcb7d20d348ad73112b3ce
Authority Key Identifier	None
CRL Distribution Points	None
Authority Information Access	None
Subject Alternative Name	None
Extended Key Usage	None
Thumbprint Algorithm	SHA1
Thumbprint	8d48db723e862f67135fc1c295cd23ab0287d172
Certificate Policies	1.3.6.1.4.1.28973.509.3.20 LVR PKI G3 Certificate Policy

LVR G3 Sub CA 01	
X.509 Version	V3
Serial Number	1657a154a196c1c7de5bd9eb03675ac6
Signature Algorithmus	sha256RSA
Signature Hash Algorithmus	sha256
Aussteller	CN = LVR G3 Root CA 01 O = Landschaftsverband Rheinland C = DE
Schlüssellänge	4096
Gültig ab	30. Oktober 2023 12:18:17
Gültig bis	31. Oktober 2020 01:59:59
Öffentlicher Schlüssel	RSA (4096 Bits)
Subject	CN = LVR G3 Sub CA 02 O = Landschaftsverband Rheinland C = DE
Schlüsselverwendung	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Subject Key Identifier	4c30a84bf5da2970dd39b1fabff9b4af98bdd19f
Authority Key Identifier	95ae0e5d5210030b3bdcb7d20d348ad73112b3ce
CRL Distribution Points	http://cdp-g3.pki.lvr.de/cdp/LVR%20G3%20Root%20CA%2001.crl
Authority Information Access	http://aia-g3.pki.lvr.de/aia/LVR%20G3%20Root%20CA%2001.crt
Subject Alternative Name	None
Extended Key Usage	None
Thumbprint Algorithm	SHA1
Thumbprint	69a00b14110b2560fa3f9866a7374c1a0ede73c8
Certificate Policies	1.3.6.1.4.1.28973.509.3.20.10.1 LVR PKI G3 Certificate Policy

LVR G3 Sub CA 02	
X.509 Version	V3
Serial Number	383cfb73cc395c490f1c16ed876bda2d
Signature Algorithmus	sha256RSA
Signature Hash Algorithmus	sha256
Issuer	CN = LVR G3 Root CA 01 O = Landschaftsverband Rheinland C = DE
Key Length	4096
Valid from	30. Oktober 2023 12:20:56
Valid to	31. Oktober 2030 01:59:59
Public Key	RSA (4096 Bits)
Subject	CN = LVR G3 Sub CA 02 O = Landschaftsverband Rheinland C = DE
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Subject Key Identifier	1932f571a3ffdcc3eacc0eeebd5f861bb34e51a7
Authority Key Identifier	95ae0e5d5210030b3bdcb7d20d348ad73112b3ce
CRL Distribution Points	http://cdp-g3.pki.lvr.de/cdp/LVR%20G3%20Root%20CA%2001.crl
Authority Information Access	http://aia-g3.pki.lvr.de/aia/LVR%20G3%20Root%20CA%2001.crt
Subject Alternative Name	None
Extended Key Usage	None
Thumbprint Algorithm	SHA1
Thumbprint	2a5ac90c96bdba8389af9a790d15904a00128ce1
Certificate Policies	1.3.6.1.4.1.28973.509.3.20.10.1 LVR PKI G3 Certificate Policy

LVR G4 Root CA 01	
X.509 Version	V3
Serial Number	1652a7bf633cfe9549a662106e6c4b53
Signature Algorithmus	sha256RSA
Signature Hash Algorithmus	sha256
Aussteller	CN = LVR G4 Root CA 01 O = Landschaftsverband Rheinland C = DE
Schlüssellänge	4096
Gültig ab	06. Mai 2025 10:53:40
Gültig bis	06. Mai 2040 11:03:11
Öffentlicher Schlüssel	RSA (4096 Bits)
Antragsteller	CN = LVR G4 Root CA 01 O = Landschaftsverband Rheinland C = DE
Schlüsselverwendung	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Subject Key Identifier	4b3cbc60bc1c5219674ad7809841cc9c94700824
Authority Key Identifier	None
CRL Distribution Points	None
Authority Information Access	None
Subject Alternative Name	None
Extended Key Usage	None
Thumbprint Algorithm	SHA1
Thumbprint	945132a35391bbb813cc9fcc50b8138b54ecf028
Certificate Policies	1.3.6.1.4.1.28973.509.4.20 LVR PKI G4 Certificate Policy

LVR G4 Sub CA 01	
X.509 Version	V3
Serial Number	2000000002d874b46afe48a3f5000000000002
Signature Algorithmus	sha256RSA
Signature Hash Algorithmus	sha256
Aussteller	CN = LVR G4 Root CA 01 O = Landschaftsverband Rheinland C = DE
Schlüssellänge	4096
Gültig ab	04. Juli 2025 11:06:16
Gültig bis	04. Juli 3032 11:16:16
Öffentlicher Schlüssel	RSA (4096 Bits)
Subject	CN = LVR G4 Sub CA 01 DC = LVRINTERN DC = LVR DC = DE
Schlüsselverwendung	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Subject Key Identifier	faf73017fb04ec46bb1bfca1ba3c37dec8ee1824
Authority Key Identifier	4b3cbc60bc1c5219674ad7809841cc9c94700824
CRL Distribution Points	http://cdp.pki.lvr.de/cdp/LVR%20G4%20Root%20CA%2001.crl
Authority Information Access	http://aia.pki.lvr.de/aia/LVR%20G4%20Root%20CA%2001.crt
Subject Alternative Name	None
Extended Key Usage	None
Thumbprint Algorithm	SHA1
Thumbprint	590eb50e0a261b27dca339d921e2ee08c2faf044
Certificate Policies	1.3.6.1.4.1.28973.509.4.20.10.1 LVR PKI G4 Certificate Policy

LVR G4 Sub CA 02	
X.509 Version	V3
Serial Number	20000000036f7ddb21c03258ca000000000003
Signature Algorithmus	sha256RSA
Signature Hash Algorithmus	sha256
Issuer	CN = LVR G4 Root CA 01 O = Landschaftsverband Rheinland C = DE
Key Length	4096
Valid from	28. Juli 2025 11:18:31
Valid to	28. Juli 2032 11:28:31
Public Key	RSA (4096 Bits)
Subject	CN = LVR G4 Sub CA 02 DC = LVRINTERN DC = LVR DC = DE
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Subject Key Identifier	a526a885e4cff77189fb799d2e235ffa6fadc103
Authority Key Identifier	4b3cbc60bc1c5219674ad7809841cc9c94700824
CRL Distribution Points	http://cdp.pki.lvr.de/cdp/LVR%20G4%20Root%20CA%2001.crl
Authority Information Access	http://aia.pki.lvr.de/aia/LVR%20G4%20Root%20CA%2001.crt
Subject Alternative Name	None
Extended Key Usage	None
Thumbprint Algorithm	SHA1
Thumbprint	2337f5d48fb2b1401dce4fadee6d200d0303ab9f
Certificate Policies	1.3.6.1.4.1.28973.509.4.20.10.1 LVR PKI G4 Certificate Policy

9.1.1 Version Nummer(s)

Die Zertifizierungsstellen der LVR PKI G3/G4 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 G3/G4 Root CA 01 • 0 für LVR G3/G4 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	LVR PKI G3 1.3.6.1.4.1.28973.509.3.20.10.1 (LVR-InfoKom CP/CPS OID Referenz)	Nein
	LVR PKI G4 1.3.6.1.4.1.28973.509.4.20.10.1 (LVR-InfoKom CP/CPS OID Referenz)	Nein

9.1.3 Algorithm Object Identifiers

Die Zertifizierungsinstanzen der LVR PKI G3/G4 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 GG3/G4 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 G3 Certificate Policy OID lautet: 1.3.6.1.4.1.28973.509.3.20.
Die LVR PKI G4 Certificate Policy OID lautet: 1.3.6.1.4.1.28973.509.4.20.

9.1.7 Policy Constraints Extension

Die Policy Constraint Extension restriktiert die Pfadlänge in der Vertrauenskette

Zertifizierungsinstanz	Länger der Vertrauenskette	Parameter
LVR G3/G4 Root CA 01	1	Path Length = 1
LVR G3/G4 Sub CA 01	0	Path Length = 0
LVR G3/G4 Sub CA 02	0	Path Length = 0

9.1.8 Policy Qualifiers Syntax und Semantik

Die LVR PKI Certificate Policy Qualifier ID ist:

- LVR PKI G3 OID: 1.3.6.1.4.1.28973.509.3.20.10.1
- LVR PKI G4 OID: 1.3.6.1.4.1.28973.509.4.20.10.1

Die LVR PKI G3/G4 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 G3/G4 ausgegeben. Eine Ausgabe von Delta CRLs ist für die LVR G4 Sub CA 01 und LVR G4 Sub CA 02 vorgesehen. Eine Ausgabe von Delta CRLs für die LVR G3/G4 Root CA 01 und LVR G3 Sub CA 01/02 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 G3 Root CA 01 – CRL Profil	
Feld	**Wert**
Version	X.509 V2
Issuer	CN = LVR G3 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	95ae0e5d5210030b3bdcb7d20d348ad73112b3ce
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 G3 Sub CA 01 – CRL Profil	
Feld	**Wert**
Version	X.509 V2
Issuer	CN = LVR G3 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	4c30a84bf5da2970dd39b1fabff9b4af98bdd19f
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 G3 Sub CA 02 – CRL Profil	
Feld	**Wert**
Version	X.509 V2
Issuer	CN = LVR G3 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	1932f571a3ffdcc3eacc0eeebd5f861bb34e51a7
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 G4 Root CA 01 – CRL Profil	
Feld	**Wert**
Version	X.509 V2
Issuer	CN = LVR G4 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	4b3cbc60bc1c5219674ad7809841cc9c94700824
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 G4 Sub CA 01 – CRL Profil	
Feld	**Wert**
Version	X.509 V2
Issuer	CN = LVR G4 Sub CA 01 DC = LVRINTERN DC = LVR DC = 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	faf73017fb04ec46bb1bfca1ba3c37dec8ee1824
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 G4 Sub CA 02 – CRL Profil	
Feld	**Wert**
Version	X.509 V2
Issuer	CN = LVR G4 Sub CA 02 DC = LVRINTERN DC = LVR DC = 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	a526a885e4cff77189fb799d2e235ffa6fadc103
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 G3/G4 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 G3/G4 Sub CA 01 und LVR G3/G4 Sub CA 02 die Sperrinformation eines Zertifikats mit maximaler 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 G3/G4 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 G3/G4 werden interne Audits (ISO 27001 Zertifizierung) durchgeführt, um Abweichungen vom Regelbetrieb der LVR G3/G4 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 G3/G4 (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 G3/G4.

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 G3/G4 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 G3/G4 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 G3/G4.

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 G3/G4 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 G3/G4 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 G3/G4zur 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 G3/G4 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%20CPCPS.pdf

11.10.2 Aufhebung

Dieses Dokument ist solange gültig, bis

- es durch eine neue Version ersetzt wird oder
- der Betrieb der
    - LVR G3/G4 Root CA 01 Zertifizierungsstelle
    - LVR G3/G4 Sub CA 01 Zertifizierungsstelle
    - LVR G3/G4 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 G3/G4 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 G3/G4 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 G3/G4 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 G3/G4.

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

Abkürzung	Definition
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