Westdeutscher Rundfunk
CPS Offline WDR-CA

Regelungen für den Zertifizierungsbetrieb

Pezhman Pedramfar Alexander Gast

21. August 2024

Westdeutscher Rundfunk
Appellhofplatz 1
D-50667 Köln

www.wdr.de

Inhaltsverzeichnis

1 Einleitung **9**
- 1.1 Überblick . . . 9
- 1.2 Name und Kennzeichnung des Dokuments . . . 10
- 1.3 Zertifikatsinfrastruktur-Teilnehmer . . . 10
  - 1.3.1 Zertifizierungsstellen . . . 10
  - 1.3.2 Registrierungsstellen . . . 10
  - 1.3.3 Zertifikatsnehmer . . . 10
  - 1.3.4 Zertifikatsnutzer . . . 10
  - 1.3.5 Weitere Teilnehmer . . . 11
- 1.4 Verwendung von Zertifikaten . . . 11
  - 1.4.1 Erlaubte Verwendung von Zertifikaten . . . 11
  - 1.4.2 Verbotene Verwendung von Zertifikaten . . . 11
- 1.5 Pflege des Policy-Dokumentes . . . 11
  - 1.5.1 Zuständigkeit für das Dokument . . . 12
  - 1.5.2 Ansprechpartner/Kontaktperson/Sekretariat . . . 12
  - 1.5.3 Pflege dieses Dokumentes . . . 12
  - 1.5.4 Annahmeverfahren für Teilnehmer-CP . . . 12
  - 1.5.5 Zuständiger für die Anerkennung einer CP in Hinblick auf diese Mindestanforderungen . . . 12
- 1.6 Begriffe und Abkürzungen . . . 13

2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen **16**
- 2.1 Verzeichnisse . . . 16
- 2.2 Veröffentlichung von Informationen zur Zertifikatserstellung . . . 16
- 2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen . . . 17
- 2.4 Zugriffskontrolle auf Verzeichnisse . . . 17

3 Identifizierung und Authentifizierung **18**
- 3.1 Namensregeln . . . 18
  - 3.1.1 Arten von Namen . . . 18
  - 3.1.2 Notwendigkeit für aussagekräftige Namen . . . 18
  - 3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern . . . 18
  - 3.1.4 Regeln für die Interpretation verschiedener Namensformen . . . 18
  - 3.1.5 Eindeutigkeit von Namen . . . 18
  - 3.1.6 Anerkennung, Authentifizierung und Rolle von Markennamen . . . 19
- 3.2 Erstmalige Überprüfung der Identität . . . 19
  - 3.2.1 Methoden zur Überprüfung des Besitzes . . . 19
  - 3.2.2 Authentifizierung von Organisationszugehörigkeiten . . . 19
  - 3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikatsnehmers 19
  - 3.2.4 Ungeprüfte Zertifikatsnehmerangaben . . . 19
  - 3.2.5 Prüfung der Berechtigung zur Antragstellung . . . 19

3.2.6 Kriterien für die Zusammenarbeit . . . 20
3.3 Identifizierung und Authentifizierung von Anträgen auf Zertifizierung nach Schlüsselerneuerung (Rekeying) . . . 20
3.3.1 Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Zertifizierung nach Schlüsselerneuerung . . . 20
3.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen 20
3.4 Identifizierung und Authentifizierung von Sperranträgen . . . 20

4 Betriebsanforderungen 21
4.1 Zertifikatsantrag . . . 21
4.1.1 Wer kann einen Zertifikatsantrag stellen? . . . 21
4.1.2 Registrierungsprozess und Zuständigkeiten . . . 21
4.2 Verarbeitung eines Zertifikatsantrags . . . 21
4.2.1 Durchführung der Identifizierung und Authentifizierung . . . 21
4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen . . . 21
4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen . . . 22
4.3 Zertifikatsausgabe . . . 22
4.3.1 Aktionen des Zertifizierungsdiensteanbieters bei der Ausgabe von Zertifikaten 22
4.3.2 Benachrichtigung des Zertfikiatsnehmers über die Ausgabe des Zertifikats durch die CA . . . 23
4.4 Zertifikatsannahme . . . 23
4.4.1 Verhalten für eine Zertifikatsannahme . . . 23
4.4.2 Veröffentlichung des Zertifikats durch die CA . . . 23
4.4.3 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe des Zertifikats . . . 23
4.5 Verwendung des Schlüsselpaares und des Zertifikats . . . 23
4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer . . . 23
4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch den Zertifikatsnutzer . . . 24
4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (certificate renewal) . 24
4.6.1 Bedingungen für eine Zertifikatserneuerung . . . 24
4.6.2 Wer darf eine Zertifikatserneuerung beantragen? . . . 24
4.6.3 Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung . . . 25
4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats . . . 25
4.6.5 Verhalten für die Annahme einer Zertifikatserneuerung . . . 25
4.6.6 Veröffentlichung der Zertifikatserneuerung durch die CA . . . 25
4.6.7 Benachrichtigung anderer Teilnehmer der PKI über die Erneuerung des Zertifikats . . . 25
4.7 Zertifikatserneuerung mit Schlüsselerneuerung . . . 25
4.7.1 Bedingungen für eine Zertifizierung nach Schlüsselerneuerung . . . 26
4.7.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen? . . . 26
4.7.3 Bearbeitung von Zertifikatsanträgen nach Schlüsselerneuerungen . . . 26
4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats . . . 26
4.7.5 Verhalten für die Annahme von Zertifikaten nach Schlüsselerneuerungen . . . 26
4.7.6 Veröffentlichung von Zertifikaten nach Schlüsselerneuerungen durch die CA . . 26

4.7.7 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe eines Nachfolgezertifikats . . . 26
4.8 Zertifikatsänderung . . . 27
4.8.1 Bedingungen für eine Zertifikatsänderung . . . 27
4.8.2 Wer darf eine Zertifikatsänderung beantragen? . . . 27
4.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung . . . 27
4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats . . . 27
4.8.5 Verhalten für die Annahme einer Zertifikatsänderung . . . 27
4.8.6 Veröffentlichung der Zertifikatsänderung durch die CA . . . 27
4.8.7 Benachrichtigung weiterer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe eines neuen Zertifikats . . . 28
4.9 Sperrung und Suspendierung von Zertifikaten . . . 28
4.9.1 Bedingungen für eine Sperrung . . . 28
4.9.2 Wer kann eine Sperrung beantragen? . . . 28
4.9.3 Verfahren für einen Sperrantrag . . . 28
4.9.4 Fristen für einen Sperrantrag . . . 29
4.9.5 Fristen/Zeitspanne für die Bearbeitung des Sperrantrags durch die WDR **RfA**-CA 29
4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen . . . 29
4.9.7 Frequenz der Veröffentlichung von Sperrlisten . . . 30
4.9.8 Maximale Latenzzeit für Sperrlisten . . . 30
4.9.9 Verfügbarkeit von Online-Sperrinformationen . . . 30
4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen . . . 30
4.9.11 Andere Formen zur Anzeige von Sperrinformationen . . . 30
4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels . . . 30
4.9.13 Bedinungen für eine Suspendierung . . . 30
4.9.14 Wer kann eine Suspendierung beantragen? . . . 31
4.9.15 Verfahren für Anträge auf Suspendierung . . . 31
4.9.16 Begrenzungen für die Dauer von Suspendierung . . . 31
4.10 Statusabfragedienst für Zertifikate . . . 31
4.10.1 Funktionsweise des Statusabfragedienstes . . . 31
4.10.2 Verfügbarkeit des Statusabfragedienstes . . . 31
4.10.3 Optionale Leistungen . . . 31
4.11 Kündigung durch den Zertifikatsnehmer . . . 31
4.12 Schlüsselhinterlegung und -wiederherstellung . . . 32
4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel . . . 32
4.12.2 Bedinungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln . . . 32

5 Nicht-technische Sicherheitsmaßnahmen **33**
5.1 Bauliche Sicherheitsmaßnahmen . . . 33
5.1.1 Lage und Gebäude . . . 33
5.1.2 Zugang . . . 33
5.1.3 Strom, Heizung und Klimaanlage . . . 33
5.1.4 Wassergefährdung . . . 33
5.1.5 Brandschutz . . . 33
5.1.6 Lager und Archiv . . . 34
5.1.7 Datenvernichtung . . . 34

5.1.8 Disaster Backup . . . 34
5.2 Verfahrensvorschriften . . . 34
5.2.1 Rollenkonzept . . . 34
5.2.2 Mehraugenprinzip . . . 38
5.2.3 Identifizierung und Authentifizierung jeder Rolle . . . 39
5.2.4 Rollentrennung . . . 39
5.3 Personelle Sicherheitsmaßnahmen . . . 39
5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit . . . 39
5.3.2 Sicherheitsüberprüfung der Mitarbeiter . . . 39
5.3.3 Anforderungen an Schulungen . . . 39
5.3.4 Häufigkeit von Schulungen und Belehrungen . . . 40
5.3.5 Häufigkeit und Folge von Job-Rotation . . . 40
5.3.6 Maßnahmen bei unerlaubten Handlungen . . . 40
5.3.7 Anforderungen an freie Mitarbeiter . . . 40
5.3.8 Dokumente, die dem Personal zur Verfügung gestellt werden müssen . . . 40
5.4 Überwachungsmaßnahmen . . . 40
5.4.1 Arten von aufgezeichneten Ereignissen . . . 40
5.4.2 Häufigkeit der Bearbeitung der Aufzeichnungen . . . 40
5.4.3 Aufbewahrungszeit von Aufzeichnungen . . . 41
5.4.4 Sicherung der Aufzeichnungen . . . 41
5.4.5 Datensicherung der Aufzeichnungen . . . 41
5.4.6 Speicherung der Aufzeichnungen (intern / extern) . . . 41
5.4.7 Benachrichtigung der Ereignisauslöser . . . 41
5.4.8 Schwachstellenanalyse . . . 41
5.5 Archivierung von Aufzeichnungen . . . 42
5.5.1 Arten von archivierten Aufzeichnungen . . . 42
5.5.2 Aufbewahrungsfristen für archivierte Daten . . . 42
5.5.3 Sicherung des Archivs . . . 42
5.5.4 Datensicherung des Archivs . . . 43
5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen . . . 43
5.5.6 Archivierung (intern / extern) . . . 43
5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen . . . 43
5.6 Schlüsselwechsel der RfA-CA . . . 43
5.7 Kompromittierung und Geschäftsweiterführung bei der RfA-CA . . . 43
5.7.1 Behandlung von Vorfällen und Kompromittierungen . . . 43
5.7.2 Rechnerressourcen-, Software- und/oder Datenkompromittierung . . . 44
5.7.3 Verhalten bei Kompromittierung des privaten Schlüssels der RfA-CA . . . 44
5.7.4 Möglichkeiten zur Geschäftsweiterführung nach einer Kompromittierung . . . 44
5.8 Schließung einer **RfA**-CA oder einer Registrierungsstelle . . . 45

6 Technische Sicherheitsmaßnahmen **46**
6.1 Erzeugung und Installation von Schlüsselpaaren . . . 46
6.1.1 Erzeugung von Schlüsselpaaren . . . 46
6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer . . . 46
6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber . . . 46
6.1.4 Lieferung öffentlicher Schlüssel der **RfA**-CA an Zertifikatsnutzer . . . 46
6.1.5 Schlüssellängen . . . 47
6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle . . . 47
6.1.7 Schlüsselverwendungen . . . 47

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module . 47
6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module 47
6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m) 47
6.2.3 Hinterlegung privater Schlüssel 48
6.2.4 Sicherung privater Schlüssel 48
6.2.5 Archivierung privater Schlüssel 48
6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen 48
6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen 48
6.2.8 Aktivierung privater Schlüssel 48
6.2.9 Deaktivierung privater Schlüssel 48
6.2.10 Zerstörung privater Schlüssel 48
6.2.11 Beurteilung kryptographischer Module 49
6.3 Andere Aspekte des Managements von Schlüsselpaaren 49
6.3.1 Archivierung öffentlicher Schlüssel 49
6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren 49
6.4 Aktivierungsdaten 49
6.4.1 Aktivierungsdaten 49
6.4.2 Schutz von Aktivierungsdaten 49
6.5 Sicherheitsmaßnahmen in den Rechneranlagen 50
6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen . . . 50
6.5.2 Beurteilung von Computersicherheit 50
6.6 Technische Maßnahmen während des Life Cycles 50
6.6.1 6.6.1 Sicherheitsmaßnahmen bei der Entwicklung 50
6.6.2 6.6.2 Sicherheitsmaßnahmen beim Computermanagement 50
6.6.3 Sicherheitsmaßnahmen während der Life Cycles 50
6.7 Sicherheitsmaßnahmen für Netze 51
6.8 Zeitstempel 51

7 Profile von Zertifikaten, Sperrlisten und OCSP 52
7.1 Zertifikatsprofile 52
7.1.1 Versionsnummern 52
7.1.2 Zertifikatserweiterungen 52
7.1.3 Algorithmen OIDs 52
7.1.4 Namensformate 52
7.1.5 Namensbeschränkungen 53
7.1.6 OIDs der Zertifikatsrichtlinien 53
7.1.7 Nutzung der Erweiterung ”Policy Constraints” 53
7.1.8 Syntax und Semantik von ”Policy Qualifiers” 53
7.1.9 Verarbeitung der Semantik der kritischen Erweiterung Zertifikatsrichtlinie . . . 53
7.2 Sperrlistenprofile 53
7.2.1 Versionsnummer(n) 53
7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen 53
7.3 Profile des Statusabfragedienstes (OCSP) 54
7.3.1 Versionsnummer(n) 54
7.3.2 OCSP Erweiterungen 54

8 Überprüfungen und andere Bewertungen 55
8.1 Häufigkeit und Bedingungen für Überprüfungen 55
8.2 Identität/Qualifikation des Prüfers 56

8.3 Stellung des Prüfers zum Bewertungsgegenstand . . . 56
8.4 Durch Überprüfungen abgedeckte Themen . . . 56
8.5 Reaktionen auf Unzulänglichkeiten . . . 56
8.6 Information über Bewertungsergebnisse . . . 56

9 Andere finanzielle und rechtliche Angelegenheiten 57
9.1 Preise . . . 57
9.2 Finanzielle Zuständigkeiten . . . 57
9.3 Vertraulichkeitsgrad von Geschäftsdaten . . . 57
9.3.1 Definition von vertraulichen Informationen . . . 57
9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören . . . 57
9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen . . . 57
9.4 Datenschutz von Personendaten . . . 58
9.4.1 Datenschutzkonzept . . . 58
9.4.2 Als persönlich behandelte Daten . . . 58
9.4.3 Daten, die nicht als persönlich behandelt werden . . . 58
9.4.4 Zuständigkeiten für den Datenschutz . . . 58
9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten . . . 58
9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften . . . 58
9.4.7 Andere Bedingungen für Auskünfte . . . 58
9.5 Geistiges Eigentumsrecht . . . 59
9.6 Zusicherungen und Garantien . . . 59
9.6.1 Zusicherungen und Garantien der CA . . . 59
9.6.2 Zusicherungen und Garantien der RA . . . 59
9.6.3 Zusicherungen und Garantien der Zertifikatsnehmer . . . 59
9.6.4 Zusicherungen und Garantien der Zertifikatsnutzer . . . 59
9.6.5 Zusicherungen und Garantien anderer Zertifikatsinfrastruktur-Teilnehmer . . . 59
9.7 Haftungsausschlüsse . . . 59
9.8 Haftungsbeschränkungen . . . 60
9.9 Schadensersatz . . . 60
9.10 Gültigkeitsdauer und Beendigung . . . 60
9.10.1 Gültigkeitsdauer . . . 60
9.10.2 Beendigung . . . 60
9.10.3 Auswirkung der Beendigung und Weiterbestehen . . . 60
9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern . . . 60
9.12 Ergänzungen . . . 60
9.12.1 Verfahren für Ergänzungen . . . 60
9.12.2 Benachrichtigungsmechanismen und –fristen . . . 61
9.12.3 Bedingungen für OID Änderungen . . . 61
9.13 Verfahren zur Schlichtung von Streitfällen . . . 61
9.14 Zugrundeliegendes Recht . . . 61
9.15 Einhaltung geltenden Rechts . . . 62
9.16 Sonstige Bestimmungen . . . 62
9.16.1 Vollständigkeitserklärung . . . 62
9.16.2 Abgrenzungen . . . 62
9.16.3 Salvatorische Klausel . . . 62
9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht) . . . 62
9.16.5 Höhere Gewalt . . . 62
9.16.6 Andere Bestimmungen . . . 62

Disclaimer

Das in diesem Dokument gewählte generische Maskulinum bezieht sich zugleich auf die männliche, die weibliche und andere Geschlechteridentitäten. Zur besseren Lesbarkeit wird auf die Verwendung männlicher und weiblicher Sprachformen verzichtet. Alle Geschlechteridentitäten werden ausdrücklich mitgemeint, soweit die Aussagen dies erfordern.

1 Einleitung

In diesem Dokument wird **RfA** (fettgedruckt) als Synonym für den **Westdeutschen Rundfunk (WDR)** verwendet.

Es bezieht sich auf die Version 3.4 der Mindestanforderungen (CP) der Rundfunk-Root-CA.

1.1 Überblick

Die **RfA**-CA und die von ihr zertifizierten **RfA** Sub-CAs sind Teil der übergreifenden Zertifikatsinfrastruktur des gesamten ARD-Netzes, die gemeinsame PKI-Anwendungen über die Grenzen einzelner Rundfunkanstalten hinweg ermöglicht. Hierzu zählen im Besonderen der RfA-übergreifende WLAN-Zugang und die RfA-übergreifende SSL/TLS-Webserver-Authentifikation. Zu diesem Zweck ist die **RfA**-CA von der Rundfunk-Root-CA zertifiziert.

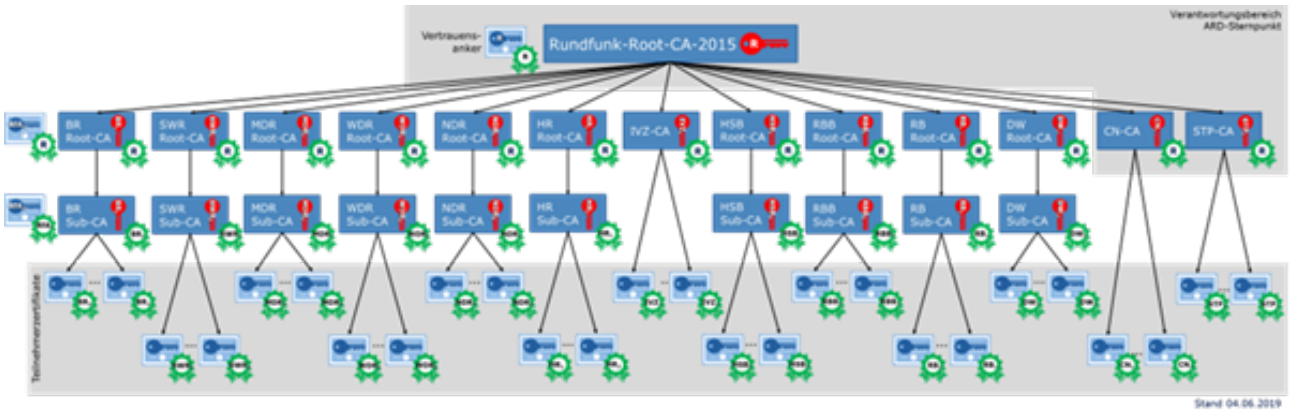

Abbildung 1.1: Beispielhafter Überblick über die Zertifikatsinfrastruktur des ARD-Netzes

Dieses Dokument ist das Certificate Practice Statement (CPS) der **RfA**-CA. Es stellt dar, wie die Mindestanforderungen der Rundfunk-Root-CA an den Zertifizierungsbetrieb von der **RfA**-CA umgesetzt werden. Alle in den Mindestanforderungen der Rundfunk-Root-CA genannten Anforderungen sind für die RfA-CAs verbindlich und können nicht abgeschwächt werden. Die Anforderungen betreffen die infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen und Abläufe innerhalb der RfA-CAs und legen dabei insbesondere die Rahmenbedingungen für die Ausstellung von Zertifikaten entsprechend der internationalen Norm X.509 fest.

In weiteren, separaten Dokumenten ist die Zertifizierungsrichtlinie (CP) und die Certificate Practice Statements (CPS) für die RfA Sub-CAs niedergelegt, die die aus den Mindestanforderungen der Rundfunk-Root-CA an den Zertifizierungsbetrieb resultierenden Vorgaben und Anforderungen an RfA Sub-CAs festlegt sowie deren Umsetzung beschreiben.

Die **RfA**-CA wird in einer Virtuellen Maschine (VM) ausschließlich offline betrieben. Bei Nichtgebrauch ist die VM heruntergefahren und das darunter liegende Notebook ausgeschaltet in einem Tresor verwahrt.

1.2 Name und Kennzeichnung des Dokuments

Name	Certificate Policy Statement (CPS) der Offline WDR-CA
Version	2.1
Datum	21. August 2024
OID	1.3.6.1.4.1.42638.1.7.2.2.1

1.3 Zertifikatsinfrastruktur-Teilnehmer

1.3.1 Zertifizierungsstellen

Der CSP betreibt die **RfA**-PKI als untergeordnete Hierarchie der Rundfunk-Root-CA. Den CAs obliegt die Ausstellung von Zertifikaten innerhalb der **RfA**-PKI. Die **RfA**-CA stellt ausschließlich Sub-CA Zertifikate aus.

1.3.2 Registrierungsstellen

Die Registrierungsstelle (**RfA**-RA) ist Bestandteil der **RfA**-CA. Zertifikatsnehmer der **RfA**-CA können nur Sub-CAs, aber keine Endanwender sein.

Da die **RfA**-CA, die **RfA**-Issuing-CAs von den gleichen Personen bei der RfA betrieben werden, ist keine gesonderte Identitätsprüfung bei der Registrierung der **RfA**-Issuing-CAs erforderlich. Für **RfA** Sub-CAs führt die Registrierungsstelle die Überprüfung der Identität und Authentizität von Zertifikatsnehmern durch, sofern eine gesonderte Identitätsprüfung erforderlich ist (siehe Kapitel 3.2.3).

1.3.3 Zertifikatsnehmer

Zertifikatsnehmer der **RfA**-CA sind ausschließlich Sub-CAs, die ein Zertifikat der **RfA**-CA erhalten.

1.3.4 Zertifikatsnutzer

Zertifikatsnutzer der **RfA**-CA sind **RfA**-interne Nutzer (Personen, Systeme und Organisationen) sowie Nutzer im ARD-Netz, die Zertifikate von Zertifikatsnehmern nutzen.

1.3.5 Weitere Teilnehmer

CA-Steuerungsgruppe
Die **RfA**-CA ist mit einem Sitz in der CA-Steuerungsgruppe vertreten. Die **RfA** hat Rainer Birkendorf (rainer.birkendorf@wdr.de) als Vertreter in der CA-Steuerungsgruppe benannt.

CA-Ansprechpartner
Die **RfA** hat dem Betreiber der Rundfunk-Root-CA Pezhman Pedramfar (pezhman.pedramfar@wdr.de) als CA-Ansprechpartner und Alexander Gast (alexander.gast@wdr.de) als Vertreter des CA-Ansprechpartners benannt. Die CA-Ansprechpartner stehen dem Betreiber der Rundfunk-Root-CA als technische Ansprechpartner zur Verfügung und beraten im Vorfeld für Themen, die von der CA-Steuerungsgruppe entschieden werden.

Die Namen und Kontaktdaten der Ansprechpartner und des Steuerungsgruppenmitgliedes befinden sich zusätzlich unter folgender URL: `https://ca.wdr.cn.ard.de`

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendung von Zertifikaten

Die **RfA**-CA stellt nur Sub-CA-Zertifikate aus. Die zu diesen Sub-CA Zertifikaten gehörenden privaten CA-Schlüssel dürfen ihrerseits nur zur Ausstellung von Endanwenderzertifikaten und Sperrlisten verwendet werden. Diese erlaubte Verwendung wird in den Sub-CA-Zertifikaten mittels der Zertifikatserweiterung KeyUsage gekennzeichnet.

Mittels der Zertifikatserweiterung Basic Constraints wird ein **RfA** Sub-CA Zertifikat als ein CA-Zertifikat gekennzeichnet.

1.4.2 Verbotene Verwendung von Zertifikaten

Die **RfA**-CA darf keine Endanwenderzertifikate ausstellen. Sie darf ihren CA-Schlüssel ausschließlich zur Zertifikats- oder Sperrlistenausstellung nutzen und darf den CA-Schlüssel nicht für andere Signaturen oder zu Verschlüsselungs- oder Authentisierungszwecken einsetzen.

1.5 Pflege des Policy-Dokumentes

Das Kapitel 10.2 kann geändert werden ohne, dass sich die Versionsnummer ändert und eine erneute Prüfung bei der Rundfunk-Root-CA erfolgen muss. Allerdings muss das Datum (Stand) angepasst werden.

1.5.1 Zuständigkeit für das Dokument

Zuständig für dieses Dokument sind Herr Pezhman Pedramfar und Herr Alexander Gast als Vertreter des Betreibers der **RfA**-CA.

1.5.2 Ansprechpartner/Kontaktperson/Sekretariat

Die Kontaktpersonen sind die PKI Administratoren der **RfA**, die auch als CA-Ansprechpartner beim Betreiber der Rundfunk-Root-CA benannt wurden. Die Namen der Ansprechpartner und des Steuerungsgruppenmitgliedes befinden sich unter folgender URL: https://ca.wdr.cn.ard.de

1.5.3 Pflege dieses Dokumentes

Dieses Dokument wird einmal im Jahr vom Betreiber der **RfA**-PKI auf Aktualität und Erhalt der Konformität zur jeweils aktuellen Fassung der Mindestanforderungen der Rundfunk-Root-CA an RfA-CAs überprüft. Eine bloße Korrektur auf sprachlicher Ebene (Schreibfehler, Grammatikfehler u. ä.) ist keine Änderung in diesem Sinne und erfordert keine formale Freigabe.

1.5.4 Annahmeverfahren für Teilnehmer-CP

Die **RfA**-CA hat dem Betreiber der Rundfunk-Root-CA bei Zertifikatsbeantragung eine Selbsterklärung und dieses CPS Dokument vorgelegt, welches darlegt, wie die Mindestanforderungen der Rundfunk-Root-CA von der **RfA**-CA umgesetzt werden.

Die Anforderungen an RfA Sub-CAs, die durch die **RfA**-CA zertifiziert werden möchten, sind in der Zertifizierungsrichtlinie für Sub-CAs (CP der **RfA** Sub-CA) auf Basis der Mindestanforderungen der Rundfunk-Root-CA niedergelegt. Alle in dieser Zertifizierungsrichtlinie genannten Anforderungen an die RfA Sub-CAs sind verbindlich und können nicht abgeschwächt werden.

Bei einer Zertifikatsbeantragung bei der **RfA**-CA muss eine RfA Sub-CA ebenfalls ein CPS Dokument vorlegen und erklären, dass sie die Anforderungen der CP der RfA Sub-CA einhält. Vor Zertifikatsausstellung prüft die **RfA**-CA die CP und CPS Dokumente der **RfA** Sub-CA. Erfüllt die RfA Sub-CA die in diesen Dokumenten beschriebenen Anforderungen für RfA Sub-CAs nicht, wird die Zertifizierung von der **RfA**-CA abgelehnt oder nachträglich widerrufen.

1.5.5 Zuständiger für die Anerkennung einer CP in Hinblick auf diese Mindestanforderungen

Zuständig für die Anerkennung der CP und CPS Dokumente einer **RfA** Sub-CA ist einer der Betreiber der **RfA**-CA (siehe 1.5.2).

1.6 Begriffe und Abkürzungen

AD	**Active Directory** Microsoft Windows Verzeichnisdienst
AD CS	**Active Directory Certificate Services** Microsoft Windows Server CA-Rolle
ARD	**Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten Deutschlands**
Backup	Sicherung des Schlüssels bzw. einer Komponente, die auch den Schlüssel beinhaltet, mit üblichen Backup-Mechanismen, die nicht speziell für Schlüssel bestimmt sind. Z. B. also das Backup einer VM
CA	**Certificaton Authority** Zertifizierungsstelle
CC	**Common Criteria** Internationaler Standard zur Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten
CNG	**Cryptographic API Next Generation** Kryptographie-Schnittstelle in Windows
CN	**Corporate Network** Unternehmensnetzwerk; hier: ARD-übergreifendes Netzwerk
CP	**Certificate Policy** Zertifizierungsrichtlinie
CPS	**Certification Practice Statement** Regelungen für den Zertifizierungsbetrieb
CRL	**Certificate Revocation List** Zertifikatssperrliste
CSR	**Certificate Signing Request** Zertifikatsantrag
DN	**Distinguished Name** Vollqualifizierter Name
DNS	**Domain Name System** System zur Namensauflösung in IP-Netzwerken
Hinterlegung	Sichere Aufbewahrung des Schlüssels (offline und/oder verschlüsselt) für ein mögliches Disaster Recovery, in der Obhut von Dritten (Tresor, Bankschließfach) für den eigenen Schlüssel der CA oder treuhänderisch für Dritte durch die CA (dann ”Key Escrow”). Die Wahrscheinlichkeit, dass auf einen hinterlegten Schlüssel zurückgegriffen werden muss, ist eher gering.
HSM	**Hardware Security Module** Hardware-Sicherheitsmodul

HTTP(S)	**Hypertext Transfer Protocol (Secure)** (Sicheres) Hypertext-Übertragungsprotokoll
IP	**Internet Protocol** Netzwerkprotokoll
LAN	**Local Area Network** Lokales Netzwerk
LDAP	**Lightweight Directory Access Protocol** Protokoll zur Abfrage/Modifikation von Informationen eines Verzeichnisdienstes
MDM	**Mobile Device Management** System zur Verwaltung von Mobilgeräten
OCSP	**Online Certificate Status Protocol** Online-Auskunftsdienst zum Status von Zertifikaten
OID	**Object Identifier** Eindeutiger Kennzeichner für Objekte
PKI	**Public Key Infrastrukture** Zertifikatsinfrastruktur (bswp. für X.509-Zertifikate)
PIN	**Personal Identification Number** Persönliche Identifikationsnummer
RADIUS	**Remote Authentication Dial-In User Service** Netzwerkprotokoll zur Authentifizierung
RfA	**Rundfunkanstalt**
SAN	**Subject Alternative Name** Weitere ”alternative” Identitäten für X.509-Zertifikate
Schlüsselinhaber	Schlüsselinhaber ist der Verfügungsberechtigte über den privaten Schlüssel, im Allgemeinen der Zertifikatsinhaber bzw. im Fall von Zertifikaten für technische Systeme der Zertifikatsverantwortliche (z. B. Serveradministrator).
Sicherung	Jede Art der Sicherung des Schlüssels zur Wiederherstellung im Bedarfsfall (i. d. R. mit Wahrscheinlichkeit höher als bei einem Disaster Recovery). Z. B. das Speichern auf einem Share verschlüsselt mit einer Passphrase im persönlichen Passwort-Safe, um den Schlüssel (und das zugehörige Zertifikat) bei Bedarf auf einem neu aufgesetzten Rechner wieder einspielen zu können.
Speicherung	Ablage des Schlüssels zum bestimmungsgemäßen Gebrauch durch den Schlüsselinhaber, ggf. auch in persistentem Speicher, sprich auf Disk, oder in einem HSM.
SSL	**Secure Socket Layer** Sicheres Übertragungsprotokoll (veraltet)
TLS	**Transport Layer Security**

	Sicheres Übertragungsprotokoll
UPN	**User Principal Name** Eindeutiges Benennungsschema von Benutzer- und Computerobjekten im AD
WDR	**Westdeutscher Rundfunk (Köln)** öffentlich rechtliche Sendeanstalt für das Bundesland Nordrhein-Westfalen
Wiederherstellung	Erneute Speicherung des Schlüssels aus Hinterlegung, Sicherung oder Backup.

2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Die **RfA**-CA stellt den Zertifikatsnutzern Sperrinformationen über Sperrlisten sowie das Rundfunk-Root-CA Zertifikat und das von der Rundfunk-Root-CA ausgestellte RfA-CA-Zertifikat sowohl im AD als auch auf Webservern für den Zugriff aus dem RfA internen LAN, Daten-CN und Internet zur Verfügung. Dafür nutzt die **RfA**-CA das vorhandene AD und dedizierte Webserver.

Die **RfA**-CA gewährleistet eine ordnungsgemäße Erbringung der o. g. Verzeichnis-Dienstleistungen im Rahmen seiner Sicherheitsrichtlinie und orientiert sich am aktuellen Stand der Technik.

Die **RfA**-CA stellt sicher, dass die Veröffentlichung personenbezogener Daten nicht den geltenden Datenschutzrichtlinien widerspricht.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

Das Root-CA Zertifikat der Rundfunk-Root-CA, das **RfA**-CA Zertifikat, sowie die Sperrliste der **RfA**-CA werden im AD der RfA verteilt und können von dort aus dem internen Netz per LDAP abgerufen werden. Das **RfA**-CA Zertifikat sowie die Sperrliste der **RfA**-CA werden zusätzlich auf einem Webserver im RfA-internen LAN veröffentlicht und können von dort aus dem internen Netz per HTTP abgerufen werden. Anwendungen, die nicht auf das AD zugreifen können, z. B. RADIUS Server oder Browser auf Nicht-Windows-Computern, können über diesen Webserver ebenfalls auf das RfA-CA-Zertifikat und deren Sperrliste zugreifen.

Damit auch alle betroffenen Systeme anderer Rundfunkanstalten die von der **RfA**-CA erstellten RfA Sub-CA Zertifikate prüfen können, werden das **RfA**-CA-Zertifikat und deren Sperrliste auch auf einem Webserver im Daten-CN veröffentlicht. Um die Integrität eines lokal vorliegenden **RfA**-CA-Zertifikats prüfen zu können, wird auf dem Webserver auch der Fingerprint des **RfA**-CA-Zertifikats veröffentlicht, der zu diesem Zweck mit dem Fingerprint des lokal vorliegenden Zertifikats verglichen werden kann. Auf einer Webseite im ARD-Netz sind auch die Ansprechpartner für die **RfA** PKI und Kontaktinformationen genannt, unter denen eine Sperrung beantragt werden kann. Außerdem ist dort dieses Policy-Dokument verfügbar.

Um auch externen Zertifikatsnutzern das **RfA**-CA Zertifikat und seine Sperrliste zur Verfügung zu stellen, wird der interne http-Verteilungspunkt mit dem Zertifikat der **RfA**-CA und deren Sperrliste zusätzlich über eine dedizierte Infrastruktur im Internet zur Verfügung gestellt. Die dort dargestellten Kontaktinformationen werden auf ein notwendiges Minimum beschränkt. Die URLs für alle oben genannten Abrufmöglichkeiten des **RfA**-CA Zertifikats und der Sperrliste werden von der **RfA**-CA in

die ausgestellten Zertifikate eingetragen. So stellt die **RfA**-CA all ihren Zertifikatsnutzern in geeigneter Weise ihre Sperrinformationen und ihre CA-Zertifikate zur Verfügung.

Informationen über die korrekte Anwendung von Kryptographie und über die Verwendung von Zertifikaten werden den Zertifikatsnehmern in geeigneter Form zur Verfügung gestellt.

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Die Veröffentlichung einer Sperrliste im AD sowie auf Webservern für den Zugriff aus dem **RfA** internen LAN, ARD-Netz und im Internet erfolgt unverzüglich, spätestens 24 Stunden nach einer durchgeführten Sperrung. Außerdem wird die Sperrliste im AD und auf den Webservern für den Zugriff aus dem **RfA** internen LAN, ARD-Netz und im Internet nach jeder regelmäßigen Ausstellung einer neuen Sperrliste durch die **RfA**-CA veröffentlicht.

Die Veröffentlichung des **RfA**-CA Zertifikats im AD und auf den Webservern für den Zugriff aus dem **RfA** internen LAN, im ARD-Netz und im Internet wird einmalig nach der Installation der **RfA**-CA ausgeführt.

Dieses Policy-Dokument der **RfA**-CA wird nach seiner Freigabe vom Betreiber der Rundfunk-Root-CA im ARD-Netz publiziert. Nach einer Aktualisierung des Dokuments wird dort die neue Version veröffentlicht.

2.4 Zugriffskontrolle auf Verzeichnisse

Der Betreiber der Verzeichnisdienste für Zertifikate und Sperrinformationen gewährleistet eine ordnungsgemäße Zugriffskontrolle, die unkontrollierte Änderungen dieser Informationen verhindert.

Der lesende Zugriff auf die im Abschnitt 2.2 genannten Informationen auf den Webservern ist ohne vorherige Anmeldung möglich. Der lesende Zugriff auf den AD-Verzeichnisdienst ist nur authentifizierten AD-Benutzern möglich. Der schreibende Zugriff ist auf berechtigte Personen beschränkt.

Zertifikate und Sperrlisten sind zum Schutz vor Manipulation durch eine digitale Signatur gesichert. Somit kann jederzeit geprüft werden, ob die Integrität der Zertifikate und Sperrlisten gewährleistet ist und ob sie von einem vertrauenswürdigen Herausgeber stammen.

3 Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

Die Namensgebung bei den Distinguished Names im `subject`- und `issuer`-Feld des CA-Zertifikats entspricht dem X.500 Standard.

3.1.2 Notwendigkeit für aussagekräftige Namen

Die von der **RfA**-CA verwendeten Namen sind aussagekräftig und identifizieren den Zertifikatsnehmer eindeutig.

Aus dem Subject Distinguished Name im **RfA**-CA Zertifikat geht der Name der Rundfunkanstalt hervor. Der Distinguished Name der **RfA**-CA lautet konform zu den Vorgaben der Rundfunk-Root-CA: `CN=WDR-CA,O=Westdeutscher Rundfunk,C=DE`

3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern

Es werden keine Pseudonyme verwendet. Die Zertifikate der **RfA**-CA werden eindeutig den Zertifikatsinhabern zugeordnet.

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Die Distinguished Names im `subject`- und `issuer`-Feld des **RfA**-CA Zertifikats und den ausgestellten **RfA** Sub-CA Zertifikaten bezeichnen den Zertifikatsinhaber und -herausgeber. Es werden keine `SubjectAltName`- und `IssuerAltName`-Erweiterungen verwendet.

3.1.5 Eindeutigkeit von Namen

Bei der Ausstellung von **RfA** Sub-CA Zertifikaten stellt die **RfA**-CA sicher, dass der Distinguished Name (DN) des Zertifikatsinhabers innerhalb der **RfA**-CA eindeutig ist.

3.1.6 Anerkennung, Authentifizierung und Rolle von Markennamen

Die **RfA**-CA ist nicht verpflichtet, Angaben von Zertifikatsinhabern auf die Einhaltung von Markenrechten, Warenzeichen usw. zu prüfen. Falls die **RfA**-CA über eine Verletzung solcher Rechte informiert wird, erfolgt die Sperrung des betroffenen Zertifikats.

3.2 Erstmalige Überprüfung der Identität

3.2.1 Methoden zur Überprüfung des Besitzes

Die **RfA**-CA weist bei der Zertifikatsbeantragung bei der Rundfunk-Root-CA den Besitz des privaten Schlüssels nach, indem der im Zertifikatantrag enthaltene Certificate Signing Request (CSR) mit dem privaten Schlüssel signiert wird. Bei Zertifikatsanträgen von **RfA** Sub-CAs verifiziert die **RfA**-CA die Signatur des Zertifikatsantrags. Sie akzeptiert nur gültig signierte Zertifikatsanträge.

3.2.2 Authentifizierung von Organisationszugehörigkeiten

Bei der Überprüfung der Identität des Antragstellers wird keine Organisationszugehörigkeit geprüft, da die **RfA** Sub-CA von den denselben Administratoren wie die **RfA**-CA betrieben wird bzw. die Antragsteller einer **RfA** Sub-CA den Administratoren der **RfA**-CA persönlich bekannt sind.

3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikatsnehmers

Bei der Zertifikatsbeantragung von einer **RfA** Sub-CA ist keine gesonderte Identitätsprüfung erforderlich, da die Authentifizierung des Antragstellers auf Basis bereits erfasster Daten erfolgt und der Antragsteller dem Betreiber der **RfA**-CA persönlich bekannt ist.

3.2.4 Ungeprüfte Zertifikatsnehmerangaben

Es werden keine ungeprüften Teilnehmerangaben in die Zertifikate von **RfA** Sub-CAs aufgenommen.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Die **RfA**-CA stellt nur Zertifikate für **RfA** Sub-CAs aus. Ein **RfA** Sub-CA-Zertifikat darf nur vom **RfA**-CA Administrator und seinem Vertreter ausgestellt werden. Bei einer Zertifikatsbeantragung für ein **RfA** Sub-CA-Zertifikat ist keine gesonderte Identitäts- und Berechtigungsprüfung erforderlich, wenn der Antragsteller den **RfA**-CA Administratoren persönlich bekannt ist. Ansonsten ist bei einem Neuantrag auf Zertifizierung eine Ausweisprüfung des Antragstellers durchzuführen.

3.2.6 Kriterien für die Zusammenarbeit

Die **RfA**-CA arbeitet nicht mit anderen Zertifikatsinfrastrukturen außerhalb der Rundfunk-Root-CA zusammen.

3.3 Identifizierung und Authentifizierung von Anträgen auf Zertifizierung nach Schlüsselerneuerung (Rekeying)

3.3.1 Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Zertifizierung nach Schlüsselerneuerung

Bei einer Zertifikatserneuerung eines **RfA** Sub-CA Zertifikats ist – wie schon beim Neuantrag (siehe Kapitel 3.2.3) – keine gesonderte Identitätsprüfung erforderlich, da der Antragsteller dem Betreiber der **RfA**-CA persönlich bekannt ist.

3.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen

Bei einer Zertifikatserneuerung nach Sperrung eines RfA Sub-CA Zertifikats ist – wie schon beim Neuantrag (siehe Kapitel 3.2.3) – keine gesonderte Identitätsprüfung erforderlich, da der Antragsteller dem Betreiber der **RfA**-CA persönlich bekannt ist.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Sperranträge dürfen von jedem gestellt werden. Bei einem Sperrantrag für eine **RfA** Sub-CA ist keine gesonderte Identitätsprüfung durch die ausstellende CA erforderlich. Eine Sperrung eines **RfA** Sub-CA Zertifikats erfolgt immer nur nach Absprache mit dem **RfA** Sub-CA Administrator bzw. seinem Vertreter.

4 Betriebsanforderungen

4.1 Zertifikatsantrag

4.1.1 Wer kann einen Zertifikatsantrag stellen?

Die **RfA**-CA stellt nur Zertifikate für RfA Sub-CAs aus. Die RfA Sub-CAs werden von denselben RfA-Administratoren betrieben wie die RfA-CA. Nur diese Administratoren können einen Zertifikatsantrag bei der **RfA**-CA stellen.

4.1.2 Registrierungsprozess und Zuständigkeiten

Eine **RfA** Sub-CA erzeugt entweder zentral oder lokal ein Schlüsselpaar. Der Zertifikatsantrag einer **RfA** Sub-CA wird auf vertrauenswürdigem Wege an die PKI Administratoren der **RfA**-CA übermittelt. Der Zertifikatsantrag enthält u.a. den öffentlichen Schlüssel der **RfA** Sub-CA und ist über die Signatur des Zertifikatsantrags gesichert.

Zulässig ist die Beantragung via E-Mail mit Rückruf an die vorab angegebene Telefonnummer des Antragstellers oder seines Vertreters zwecks Abgleich des Fingerprints des Zertifikatsantrags (CSR) oder die persönliche Übergabe eines Transfer-Datenträgers mit dem Zertifikatsantrag. Im Fall der persönlichen Übergabe muss eine Ausweisprüfung erfolgen, sofern der Antragsteller nicht persönlich bekannt ist.

Zentral erzeugte Schlüssel werden ausschließlich auf den HSM-Modulen erzeugt. Die Übertragung der privaten Schlüssel erfolgt ausschließlich verschlüsselt.

4.2 Verarbeitung eines Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Bei einer Zertifikatsbeantragung durch eine **RfA** Sub-CA ist keine gesonderte Identitätsprüfung erforderlich, da der Antragsteller den Betreibern der **RfA**-CA persönlich bekannt ist (siehe Kapitel 3.2.3).

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Die Betreiber der **RfA**-CA entscheiden nach Vorlage eines Zertifikatsantrags einer **RfA** Sub-CA über die Annahme oder Ablehnung des Antrags. Hierfür prüfen sie den Zertifikatsantrag inklusive der Si-

gnatur und das CPS Dokument der antragstellenden **RfA** Sub-CA, ob die Anforderungen aus dem CP Dokument für **RfA** Sub-CAs von der **RfA** Sub-CA erfüllt werden.

Bei der Prüfung des Zertifikatsantrags werden besonders die folgenden Punkte überprüft:

- Korrektheit des beantragten `Distinguished Name` der **RfA** Sub-CA im Feld `Subject`.
- Die Schlüssellänge muss mindestens 4096 Bits betragen für RSA
- Für ECC wird eine der Kurven P-256, P-384 oder P-521 verwendet.
- Das Attribut `Certificate Extensions` im Zertifikatsantrag (CSR) muss die folgenden Angaben zu Erweiterungen enthalten:
  - `Basic Constraints`: Critical, Subject Type = CA
  - `Key Usage`: Critical, Certificate Signing, Off-line CRL Signing, CRL Signing

Zertifikatsanträge werden nur gemäß X.509-Standard akzeptiert, die syntaktisch korrekt sind und alle erforderlichen Informationen im Antrag enthalten.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Die Bearbeitungsdauer für Zertifikatsanträge von **RfA** Sub-CAs ist nicht festgelegt, die Zertifikatsanträge werden aber wie alle anderen Anträge zeitnah bearbeitet.

4.3 Zertifikatsausgabe

4.3.1 Aktionen des Zertifizierungsdiensteanbieters bei der Ausgabe von Zertifikaten

Die Ausstellung eines **RfA** Sub-CA Zertifikats erfolgt nur im Vier-Augen-Prinzip. Die beiden CA-Administratoren der **RfA**-CA lassen sich das Notebook und die erforderlichen Unterlagen (Smartcards, Zugangsdaten, PINs) von den Tresorverwaltern geben und aktivieren darauf die VM mit der Offline CA. Die erforderlichen Passworthälften für den Betrieb der **RfA**-CA sind in versiegelten Umschlägen auf die Tresore verteilt. Die Entnahme der Objekte aus den Tresoren werden protokolliert.

Die Ausstellung und Ausgabe von **RfA** Sub-CA Zertifikaten erfolgt nur für angenommene, gültige und gemäß Kapitel 4.2 geprüfte Zertifikatsanträge, die syntaktisch korrekt sind und alle erforderlichen Informationen im Antrag enthalten. Ansonsten wird der Antrag abgelehnt. Die eindeutige Verbindung zwischen dem beantragenden Zertifikatsnehmer und dem Schlüsselpaar wird durch Verifikation der digitalen Signatur des Zertifikatsantrags mit dem privaten Schlüssel der **RfA** Sub-CA gewährleistet (siehe Abschnitt 3.2.1). Es werden nur gültig signierte Zertifikatsanträge akzeptiert. Ein Zertifikatsantrag wird nur auf vertrauenswürdigem Wege an die Betreiber der **RfA**-CA übermittelt (siehe Kap. 4.1.2), so dass die Identität des Antragstellers sichergestellt ist.

Nach Ausstellung eines **RfA** Sub-CA Zertifikats wird ein manuelles Backup der **RfA**-CA Datenbank und der Log-Dateien erstellt. Der Ausführende der **RfA**-CA kopiert die Backup-Daten auf einen Datenträger und übergibt diesen Datenträger anschließend dem zuständigen Tresorverwalter, der ihn im Tresor 3 in der **RfA** verwahrt.

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

Es findet keine gesonderte Benachrichtigung der **RfA** Sub-CA über die Ausgabe des **RfA** Sub-CA Zertifikats statt, da die ausführenden Personen auch für den Betrieb der **RfA** Sub-CAs zuständig sind.

4.4 Zertifikatsannahme

4.4.1 Verhalten für eine Zertifikatsannahme

Es gibt keinen dedizierten Prozess zur Zertifikatsannahme durch die Betreiber einer **RfA** Sub-CA. Grundsätzlich ist der Zertifikatnehmer verpflichtet, die Korrektheit des eigenen Zertifikats sowie des Zertifikats der ausstellenden CA nach Erhalt zu verifizieren.

4.4.2 Veröffentlichung des Zertifikats durch die CA

Die von der **RfA**-CA ausgestellten Zertifikate werden im **RfA**-AD sowie auf Webservern für den Zugriff aus dem **RfA**-internen LAN und dem ARD-Netz sowie im Internet bereitgestellt. Die Veröffentlichung der Zertifikate erfolgt wie im Kapitel 2 beschrieben.

4.4.3 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe des Zertifikats

Es findet keine Benachrichtigung weiterer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe eines neuen **RfA** Sub-CA Zertifikats statt.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Die **RfA**-CA verwendet ihren Schlüssel und ihr Zertifikat nur für die im Zertifikat genannten Verwendungszwecke d. h. zur Ausstellung von **RfA** Sub-CA Zertifikaten und Sperrlisten.

Der private Schlüssel der **RfA**-CA liegt auf einer primären Smartcard und drei Ersatzkarten vor, und kann nur durch Eingabe der zugehörigen PIN verwendet werden. Bei Nichtverwendung dieser Karten, werden sie in einem Tresor aufbewahrt.

Die Nutzung des Schlüssels und des Zertifikats erfolgt nur in Übereinstimmung mit der CP der Rundfunk-Root-CA. Die **RfA**-CA stellt unverzüglich einen Sperrantrag bei der Rundfunk-Root-CA,

wenn die Angaben ihres **RfA**-CA Zertifikats nicht mehr korrekt sind oder wenn ihr privater Schlüssel abhandengekommen ist, gestohlen oder möglicherweise kompromittiert wurde.

Die **RfA**-CA bietet keine Schlüsselhinterlegung für private Schlüssel von **RfA** Sub-CAs an.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch den Zertifikatsnutzer

Die **RfA**-CA wird für die im Zertifikat genannten Verwendungszwecke, d. h. zur Ausstellung von **RfA** Sub-CA Zertifikaten und Sperrlisten, verwendet.

4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (certificate renewal)

Bei einer Zertifikatserneuerung ohne Schlüsselwechsel wird einem Zertifikatsnehmer durch die zuständige CA ein neues Zertifikat unter Beibehaltung des alten Schlüsselpaars ausgestellt, sofern das Schlüsselpaar den aktuellen kryptographischen Mindestanforderungen der Rundfunk-Root-CA genügt, die im Zertifikat enthaltenen Informationen unverändert bleiben und kein Verdacht auf Kompromittierung des privaten Schlüssels vorliegt.

Im Fall einer Zertifikatserneuerung für die **RfA**-CA erfolgt eine Schlüsselerneuerung.

4.6.1 Bedingungen für eine Zertifikatserneuerung

Wenn die Gültigkeit des **RfA**-CA eigenen Zertifikats abläuft, findet keine Zertifikatserneuerung unter Beibehaltung des alten **RfA**-CA Schlüssels statt, sondern mit dem Antrag auf Erneuerung des **RfA**-CA Zertifikats werden auch immer neue Schlüssel erzeugt. Dies gilt insbesondere auch dann, wenn das CA-Zertifikat wegen Verdacht auf Kompromittierung des privaten Schlüssels gesperrt wurde oder wenn es den aktuellen kryptographischen Mindestanforderungen der Rundfunk-Root-CA nicht mehr genügt (siehe Abschnitt 4.7).

Eine **RfA** Sub-CA, deren Zertifikat abläuft, ist – sofern sie ihren Betrieb weiterhin aufrechterhalten will – verpflichtet, rechtzeitig eine Zertifikatserneuerung mit oder ohne Schlüsselwechsel zu beantragen. Falls eine **RfA** Sub-CA eine Zertifikatserneuerung ohne Schlüsselwechsel beantragt, wird eine Zertifikatserneuerung ohne Schlüsselwechsel verweigert, wenn deren CA-Zertifikat wegen Verdacht auf Kompromittierung des privaten Schlüssels gesperrt wurde oder es den aktuellen kryptographischen Mindestanforderungen der Rundfunk-Root-CA nicht mehr genügt. In dem Fall muss eine Schlüssel- und Zertifikatserneuerung stattfinden (siehe Abschnitt 4.7).

4.6.2 Wer darf eine Zertifikatserneuerung beantragen?

Eine Zertifikatserneuerung für das Zertifikat der **RfA**-CA wird von den benannten Administratoren der **RfA**-CA bei der Rundfunk-Root-CA beantragt. Ein Antrag auf Zertifikatserneuerung für das Zerti-

fikat einer **RfA** Sub-CA wird von den Betreibern der **RfA**-CA nur von einem der benannten Administratoren der **RfA** Sub-CA akzeptiert, anderenfalls wird der Antrag abgelehnt.

4.6.3 Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung

Einen Antrag auf Zertifikatserneuerung von einer **RfA** Sub-CA prüft die **RfA**-CA daraufhin, ob das vorhandene Zertifikat der **RfA** Sub-CA gesperrt wurde und ob die aktuellen kryptographischen Mindestanforderungen der Rundfunk-Root-CA verletzt werden. Bei positiver Prüfung weist sie den Antrag auf Zertifikatserneuerung zurück, da auch der Schlüssel der **RfA** Sub-CA erneuert werden muss. Im anderen Fall wird das beantragte Zertifikat erstellt. Die Bearbeitung der Anträge auf Zertifikatserneuerung entspricht den Regelungen unter Abschnitt 4.2. Für die Identifizierung und Authentifizierung gelten die Regelungen gemäß Abschnitt 3.2.

4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Es muss keine zusätzliche Benachrichtigung bzgl. der Zertifikatserstellung stattfinden.

4.6.5 Verhalten für die Annahme einer Zertifikatserneuerung

Es gibt keinen dedizierten Prozess zur Annahme des Zertifikats nach einer Schlüsselerneuerung (wie auch bei einer Neubeantragung, siehe Abschnitt 4.4.1).

4.6.6 Veröffentlichung der Zertifikatserneuerung durch die CA

Es gelten die gleichen Regelungen wie bei einer Neubeantragung (siehe Abschnitt 4.4.2).

4.6.7 Benachrichtigung anderer Teilnehmer der PKI über die Erneuerung des Zertifikats

Eine Benachrichtigung ist nicht vorgesehen.

4.7 Zertifikatserneuerung mit Schlüsselerneuerung

Bei einer Zertifikatserneuerung mit Schlüsselwechsel wird einem Zertifikatsnehmer, der bereits ein Zertifikat besitzt, durch die zuständige **RfA**-CA ein neues Zertifikat für ein neues Schlüsselpaar ausgestellt, sofern die im Zertifikat enthaltenen Informationen unverändert bleiben. Es wird analog zu Abschnitt 4.6 vorgegangen.

4.7.1 Bedingungen für eine Zertifizierung nach Schlüsselerneuerung

Eine Zertifikatserneuerung der **RfA**-CA mit Schlüsselwechsel muss bei der Rundfunk-Root-CA beantragt werden, wenn z. B. die Gültigkeit eines Zertifikats abläuft. Sie muss auch beantragt werden, wenn ein Zertifikat aufgrund von Schlüsselkompromittierung gesperrt wurde.

Eine Zertifikatserneuerung einer **RfA** Sub-CA mit Schlüsselwechsel kann beantragt werden, wenn z. B. die Gültigkeit eines Sub-CA-Zertifikats abläuft. Sie muss zwingend beantragt werden, wenn ein Zertifikat aufgrund von Schlüsselkompromittierung gesperrt wurde.

4.7.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen?

Es gelten die gleichen Regelungen wie bei einer Neubeantragung, siehe Abschnitt 4.1.

4.7.3 Bearbeitung von Zertifikatsanträgen nach Schlüsselerneuerungen

Die Bearbeitung der Anträge auf Schlüssel- und Zertifikatserneuerung von **RfA** Sub-CAs entspricht den Regelungen unter Abschnitt 4.2. Für die Identifizierung und Authentifizierung gelten die Regelungen gemäß Abschnitt 3.2.

4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Die Betreiber einer **RfA** Sub-CA werden von dem Betreiber der **RfA**-CA nicht auf den Ablauf ihres CA-Zertifikats und eine notwendige Zertifikatserneuerung hingewiesen. Es findet auch keine Benachrichtigung der **RfA** Sub-CA über die Ausgabe eines Nachfolgezertifikats statt (wie auch bei einer Neubeantragung, siehe Abschnitt 4.3.2).

4.7.5 Verhalten für die Annahme von Zertifikaten nach Schlüsselerneuerungen

Es gibt keinen dedizierten Prozess zur Annahme des Zertifikats nach einer Schlüsselerneuerung (wie auch bei einer Neubeantragung, siehe Abschnitt 4.4.1).

4.7.6 Veröffentlichung von Zertifikaten nach Schlüsselerneuerungen durch die CA

Es gelten die gleichen Regelungen wie bei einer Neubeantragung (siehe Abschnitt 4.4.2).

4.7.7 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Es findet keine Benachrichtigung weiterer Instanzen statt (wie auch bei einer Neubeantragung, siehe Abschnitt 4.4.3).

4.8 Zertifikatsänderung

4.8.1 Bedingungen für eine Zertifikatsänderung

Eine Zertifikatsänderung wird von der **RfA**-CA oder einer **RfA** Sub-CA bei der ausstellenden CA beantragt, wenn sich Angaben im CA-Zertifikat geändert haben. Technisch bedeutet dies die Sperrung des alten Zertifikats und die Ausstellung eines neuen Zertifikats.

4.8.2 Wer darf eine Zertifikatsänderung beantragen?

Es gelten die gleichen Regelungen wie bei einer Neubeantragung, siehe Abschnitt 4.1

4.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung

EDie Bearbeitung der Anträge auf Zertifikatsänderung entspricht den Regelungen unter Abschnitt 4.2. Für die Identifizierung und Authentifizierung gelten die Regelungen gemäß Abschnitt 3.2.

Eine Zertifikatsänderung bedeutet technisch die Sperrung eines Zertifikats und die Ausstellung eines neuen Zertifikats mit den geänderten Zertifikatsinhalten.

Wird von einer **RfA** Sub-CA eine Zertifikatsänderung bei der **RfA**-CA beantragt, sperrt die **RfA**-CA das bestehende Zertifikat der betreffenden **RfA** Sub-CA und stellt ein neues **RfA** Sub-CA Zertifikat aus. Für den Ablauf gelten die gleichen Regelungen wie in den Abschnitten 4.9 und 4.7 bzw. 4.6 beschrieben.

4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Die Betreiber einer **RfA** Sub-CA werden von dem Betreiber der **RfA**-CA nicht über die Ausgabe eines neuen Zertifikats benachrichtigt.

4.8.5 Verhalten für die Annahme einer Zertifikatsänderung

Es gibt keinen dedizierten Prozess zur Annahme einer Zertifikatsänderung.

4.8.6 Veröffentlichung der Zertifikatsänderung durch die CA

Es gelten die gleichen Regelungen wie bei einer Neubeantragung, d. h. die **RfA**-CA veröffentlicht gemäß Abschnitt 4.4.2.

4.8.7 Benachrichtigung weiterer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe eines neuen Zertifikats

Es findet keine Benachrichtigung weiterer Zertifikatsinfrastruktur-Teilnehmer statt.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Bedingungen für eine Sperrung

Die **RfA**-CA beantragt den Widerruf ihres eigenen **RfA**-CA Zertifikats bei der Rundfunk-Root-CA, wenn mindestens einer der folgenden Fälle eintritt:

- Das Zertifikat enthält Angaben, die nicht (mehr) gültig sind.
- Der private Schlüssel der **RfA**-CA wurde verloren, gestohlen, offengelegt oder anderweitig kompromittiert beziehungsweise missbraucht.
- Der Zertifikatsnehmer (die **RfA**-CA) ist nicht mehr berechtigt, das Zertifikat zu benutzen.
- Der Zertifikatsnehmer (die **RfA**-CA) hält die CP, d. h. die Mindestanforderungen der Rundfunk-Root-CA nicht ein.
- Die **RfA**-CA hält die Regelungen dieses CPS Dokuments nicht ein; somit müssen auch die **RfA** Sub-CA-Zertifikate gesperrt werden.
- Die **RfA**-CA stellt den Zertifizierungsbetrieb ein.
- Der Zertifikatsnehmer (die **RfA**-CA) benötigt das Zertiifkat aus anderen Gründen nicht mehr.

4.9.2 Wer kann eine Sperrung beantragen?

Die Sperrung des **RfA**-CA Zertifikats oder des Zertifikats einer **RfA** Sub-CA darf grundsätzlich von jedermann beantragt werden.

Insbesondere die CA-Administratoren der **RfA**-CA und der Informationssicherheitsbeauftragte der **RfA** sind verpflichtet, eine Sperrung des Zertifikats der **RfA**-CA bei der Rundfunk-Root-CA zu beantragen, wenn ihnen ein hinlänglicher Sperrgrund bekannt wird.

4.9.3 Verfahren für einen Sperrantrag

Bei Verdacht auf Kompromittierung des **RfA**-CA Schlüssels oder bei Einstellung des Betriebes der **RfA**-CA stellt der CA-Administrator der **RfA**-CA oder sein Vertreter einen Sperrantrag bei der Rundfunk-Root-CA. Werden Mindestanforderungen der Rundfunk-Root-CA nicht eingehalten, kann auch der Informationssicherheitsbeauftragte einen Sperrantrag bei der Rundfunk-Root-CA stellen. Daneben kann auch jeder andere, dem ein entsprechender Sachverhalt bekannt wird, einen Antrag auf Sperrung der **RfA**-CA bei der Rundfunk-Root-CA stellen, der nach den Vorgaben der Rundfunk-Root-CA geprüft und ggf. umgesetzt wird.

Bei Verdacht auf Kompromittierung eines **RfA** Sub-CA Schlüssels oder bei Einstellung des Betriebs einer RfA Sub-CA, ist der Betreiber der **RfA** Sub-CA verpflichtet, einen Sperrantrag bei der **RfA**-CA

zu stellen. Hierüber wird eine Protokollnotiz angefertigt und im jahresbezogenen Excel-Protokoll auf dem verschlüsselten Laufwerk der **RfA** PKI abgelegt und dort archiviert.

Das Verfahren zur Sperrung eines **RfA** Sub-CA Zertifikats ist den Zertifikatsnehmern der **RfA**-CA bekannt, da eine **RfA** Sub-CA von denselben Administratoren betrieben wie die **RfA**-CA und zudem den CA-Administratoren einer **RfA** Sub-CA dieses CPS Dokument und das CP Dokument für **RfA** Sub-CAs zur Verfügung gestellt werden muss (siehe Kapitel 5.3.8).

Wird bei der **RfA**-CA ein Sperrantrag von einer RfA Sub-CA eingereicht, ist keine gesonderte Identitätsprüfung durch die **RfA**-CA erforderlich, da der Antragsteller dem Betreiber der **RfA**-CA persönlich bekannt ist. Die **RfA** Sub-CA wird von denselben Administratoren betrieben wie die **RfA**-CA.

Daneben kann auch jeder andere, dem ein entsprechender Sachverhalt bekannt wird, einen Antrag auf Sperrung einer RfA Sub-CA bei der **RfA**-CA stellen. In diesem Fall prüft einer der Administratoren der **RfA**-CA unverzüglich den gemeldeten Sachverhalt und entscheidet, ob der Sperrantrag berechtigt ist. In Zweifelsfällen können die Administratoren der **RfA**-CA dabei Rücksprache mit dem Informationssicherheitsbeauftragten der **RfA** halten. Bei einem positiven Entscheid wird das Zertifikat der **RfA** Sub-CA gesperrt. In allen Fällen erstellt der prüfende CA-Administrator der **RfA**-CA eine schriftliche Protokollnotiz über den Sperrantrag, dessen Prüfung und den Entscheid an und legt sie im jahresbezogenen Excel-Protokoll auf dem verschlüsselten Laufwerk der der RfA PKI ab.

Nach der Sperrung eines RfA Sub-CA Zertifikats und der Ausstellung einer neuen Sperrliste fertigt der durchführende CA-Administrator der **RfA**-CA eine schriftliche Protokollnotiz über den Vorgang an. Diese Protokollnotiz wird in einem Dokumentationsort angeben der **RfA** PKI abgelegt und dort archiviert.

Abschließend wird eine neue Sperrliste der **RfA**-CA ausgestellt und im **RfA**-AD, **RfA**-internen LAN und ARD-Netz sowie im Internet publiziert.

4.9.4 Fristen für einen Sperrantrag

Bei Bekanntwerden eines Sperrgrundes beantragt die **RfA**-CA unverzüglich die Sperrung ihres Zertifikats bei der Rundfunk-Root-CA.

4.9.5 Fristen/Zeitspanne für die Bearbeitung des Sperrantrags durch die WDR RfA-CA

Wird bei der **RfA**-CA ein Antrag auf Zertifikatssperrung eingereicht, erfolgt unverzüglich die Bearbeitung des Sperrantrags.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Die **RfA**-CA stellt den Zertifikatsprüfern intern, im ARD-Netz und im Internet, Sperrinformationen zu den von ihr ausgestellten Zertifikaten in Form von Sperrlisten zur Verfügung.

4.9.7 Frequenz der Veröffentlichung von Sperrlisten

Die Sperrliste der **RfA**-CA wird alle 12 Monate neu ausgestellt und ist 13 Monate lang gültig. Somit ergibt sich ein Monat Karenz für die manuelle Erstellung der nächsten Sperrliste. Im Fall der Sperrung oder Ausstellung eines Zertifikats wird bereits früher eine neue Sperrliste ausgestellt, die auch wieder für 13 Monate gültig ist.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die maximale Latenzzeit für Sperrlisten (Zeitpuffer zwischen planmäßiger Erstellung und spätester Veröffentlichung einer neuen Sperrliste) beträgt einen Monat.

4.9.9 Verfügbarkeit von Online-Sperrinformationen

Die **RfA**-CA bietet keinen generellen Online-Dienst zur Auskunft (OCSP) der Gültigkeit von **RfA** Sub-CA Zertifikaten an.

4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen

Bei der WDR **RfA**-CA bestehen keine Anforderungen an Online-Statusabfragen.

Bestehende Anforderungen an Online-Statusabfragen für Zertifikate einer WDR Sub-CA müssen in dem jeweilig zugehörigen CPS- beziehungsweise kombinierten CP/CPS-Dokument festgehalten werden.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Es gibt bei der **RfA**-CA keine weiteren Formen zur Anzeige von Sperrinformationen bzw. der Widerrufsbekanntmachung.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Bei Kompromittierung des privaten Schlüssels der **RfA**-CA wird unverzüglich ein Sperrantrag bei der Rundfunk-Root-CA gestellt. Bei einem Sperrantrag einer **RfA** Sub-CA wegen Kompromittierung ihres privaten Schlüssels wird das zugehörige Zertifikat unverzüglich von der **RfA**-CA widerrufen und umgehend – auch außerhalb des regulären Rhythmus – eine neue Sperrliste veröffentlicht.

4.9.13 Bedinungen für eine Suspendierung

Eine temporäre Sperrung bzw. eine Suspendierung von Zertifikaten ist bei der **RfA**-CA verboten.

4.9.14 Wer kann eine Suspendierung beantragen?

Eine Suspendierung von Zertifikaten ist bei der **RfA**-CA verboten.

4.9.15 Verfahren für Anträge auf Suspendierung

Eine Suspendierung von Zertifikaten ist bei der **RfA**-CA verboten.

4.9.16 Begrenzungen für die Dauer von Suspendierung

Eine Suspendierung von Zertifikaten ist bei der **RfA**-CA verboten.

4.10 Statusabfragedienst für Zertifikate

Die **RfA**-CA bietet keinen Statusabfragedienst an (siehe Abschnitt 4.9.9).

4.10.1 Funktionsweise des Statusabfragedienstes

Die **RfA**-CA bietet keinen Statusabfragedienst an (siehe Abschnitt 4.9.9).

4.10.2 Verfügbarkeit des Statusabfragedienstes

Die **RfA**-CA bietet keinen Statusabfragedienst an (siehe Abschnitt 4.9.9).

4.10.3 Optionale Leistungen

Die **RfA**-CA bietet keinen Statusabfragedienst an (siehe Abschnitt 4.9.9).

4.11 Kündigung durch den Zertifikatsnehmer

Falls eine Organisationseinheit der RfA aufgelöst wird, die eine **RfA** Sub-CA betreibt, und der CA-Betrieb nicht geregelt an eine andere Organisationseinheit der RfA übergeben werden kann, sperrt die **RfA**-CA das betreffende Sub-CA Zertifikat.

4.12 Schlüsselhinterlegung und -wiederherstellung

*Die Schlüsselhinterlegung für die **RfA**-PKI wird als Anlegen einer Sicherungskopie für einen kryptografischen Schlüssel definiert. Müssen Schlüssel archiviert werden, so sind diese grundsätzlich direkt nach der Erzeugung in das Archiv einzustellen. Eine gesonderte Sicherung ist dann nicht mehr erforderlich.*

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel

Die **RfA**-CA bietet keine Schlüsselhinterlegung für **RfA** Sub-CAs an.

4.12.2 Bedinungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Es werden keine Sitzungsschlüssel verwendet.

5 Nicht-technische Sicherheitsmaßnahmen

Die Gewährleistung geeigneter infrastruktureller, organisatorischer und personeller Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb der RfA-CA. Diese Sicherheitsmaßnahmen werden nachfolgend beschrieben.

5.1 Bauliche Sicherheitsmaßnahmen

5.1.1 Lage und Gebäude

Die virtuelle Maschine der **RfA**-CA wird auf einem Notebook betrieben, das bei Nichtgebrauch sicher in Tresor 1 verwahrt wird. Die zugehörigen Smartcards werden ebenfalls in Tresoren aufbewahrt.

5.1.2 Zugang

Das Notebook mit der virtuelle Maschine der **RfA**-CA befindet sich nicht in einem Serverraum, sondern wird in einem Tresor sicher verwahrt. Der Zugriff auf diesen Tresor ist nur für berechtigte Mitarbeiter möglich. Mitarbeiter von Fremdfirmen haben keinen Zugriff darauf.

5.1.3 Strom, Heizung und Klimaanlage

Die Stromversorgung ist für den Betrieb der **RfA**-CA sichergestellt. Eine Klimatisierung ist nicht erforderlich, da die **RfA**-CA nicht in einem Serverraum betrieben wird.

5.1.4 Wassergefährdung

Gefährdungen durch Wasser ist in den Räumen, in denen das System der **RfA**-CA gelagert und bei Bedarf betrieben wird, hinreichend ausgeschlossen.

Notfallmaßnahmen können ergriffen werden.

5.1.5 Brandschutz

In den Räumen, in denen das System der **RfA**-CA gelagert und bei Bedarf betrieben wird, ist ein geeigneter Brandschutz vorhanden.

Die Büroräume sind gemäß der gültigen Brandschutzvorschriften abgesichert, bei einer Detektion des Brandschutzsystems wird automatisch die Feuerwehr alarmiert.

Die Disaster-Recovery-Tresore (vgl. Abschnitt 5.1.8) befinden sich in anderen Brandschutzabschnitten, als die Tresore zur Aufbewahrung des Hauptsystems. Zudem sind die Tresore feuersicher ausgelegt.

5.1.6 Lager und Archiv

Datenträger mit sicherheitsrelevanten, vertraulichen oder personenbezogenen Daten werden vor unberechtigten Zugriffen geschützt in verschiedenen Tresoren aufbewahrt. Die Tresore sind feuersicher ausgelegt und befinden sich in verschiedenen Häusern der **RfA**. Sie sind somit in jeweils anderen Brandschutzabschnitten und von den Serverräumen getrennt.

5.1.7 Datenvernichtung

Bei der Entsorgung von Papierdokumenten und elektronischen Datenträgern der **RfA**-CA ist sichergestellt, dass alle sicherheitsrelevanten, vertraulichen oder personenbezogenen Daten vernichtet werden. Diese werden bei einem Dienstleister unter Einhaltung der Auflagen des Datenschutzes entsorgt.

5.1.8 Disaster Backup

Zu Disaster-Recovery-Zwecken exisiteren

- drei Ersatz-Smartcards der RfA-CA,
- Sicherungskopien der **RfA**-CA Datenbank und Log-Dateien,
- eine VeraCrypt Rescue Disk sowie
- die versiegelten Passwortbriefe mit
- dem Passwort für den hinterlegten Schlüssel und
- dem Passwort für den lokalen System-Administrator des Servers der **RfA**-CA

Alle zum Betrieb der **RfA**-CA benötigten Objekte sind auf vier Tresore aufgeteilt, sodass ein Weiterbetrieb der CA bei Verlust von bis zu zwei Tresoren möglich sein sollte.

Diese Tresore sind derzeit auf zwei Gebäude aufgeteilt, in unterschiedlichen Etagen und und Brandschutzabschnitt. Zudem sind die mindestens Disaster-Recovery-Tresore feuersicher.

5.2 Verfahrensvorschriften

5.2.1 Rollenkonzept

Für Installation, Konfiguration, Betrieb und Wiederherstellung aus dem Backup der **RfA**-CA sind die folgenden Rollen definiert und umgesetzt:

Lokaler Administrator der RfA Root-CA VM

Kürzel	LA
Rollen-Typ	Betriebssystem
Mindest-Anzahl Personen	2
Aufgabe der Rolle	- Installation, Konfiguration, Administration und Wartung des Betriebssystems der **RfA**-CA - Installation der AD Certificate Services - lokale Administrationsrechte - Kenntnis der Boot- und Administrator-Passwörter der Systeme - ggf. Erneuerung des lokalen Root-CA Zertifikats (erfordert Zugriff auf den Local Machine Certificate Store)
Derzeitige Besetzung	Pezhman Pedramfar Alexander Gast

Zertifizierungsstellen-Administrator

Kürzel	CCA1
Rollen-Typ	PKI
Mindest-Anzahl Personen	2
Aufgabe der Rolle	- Konfiguriert und wartet die **RfA**-CA - konfiguriert Veröffentlichungspunkte der CA - konfiguriert die Richtlinien- und Veröffentlichungsmodule (Policy- und Exit-Module) - definiert für jeden Zertifikatsmanager die globalen Gruppen für die er zuständig ist - definiert Zertifikatsmanager - definiert weitere CA Administratoren - löschen einzelner CA-Datenbank-Records der **RfA**-CA - aktivieren, veröffentlichen und konfigurieren der CRL der **RfA**-CA - CA Konfiguration, lesen und für aktivierte Bereiche ändern - starten und stoppen des Zertifikats-Dienstes - Aktivierung der Konfiguration der Audit-Parameter
Derzeitige Besetzung	Pezhman Pedramfar Alexander Gast

Zertifikats-Manager

Kürzel	CM
Rollen-Typ	PKI
Mindest-Anzahl Personen	2
Aufgabe der Rolle	- Entgegennahme von Zertifikat- und Sperranträgen für **RfA** Sub-CAs - Zertifikats-Ausstellung und -Sperrung von **RfA** Sub-CAs - Pflege des Logbuchs
Derzeitige Besetzung	Pezhman Pedramfar Alexander Gast

Backup-Operator

Kürzel	BO
Rollen-Typ	Betriebssystem
Mindest-Anzahl Personen	2
Aufgabe der Rolle	- Erstellen und Überprüfen regelmäßiger Datensicherungen - Wiederherstellung der Umgebung aus vorhandenen Sicherungen
Derzeitige Besetzung	Pezhman Pedramfar Alexander Gast

Informationssicherheits-Beauftragter

Kürzel	ISO
Rollen-Typ	PKI / Organisation
Mindest-Anzahl Personen	1
Aufgabe der Rolle	- Durchführung oder Beauftragung betriebsinterner Audits - Durchführung oder Beauftragung der Audits von **RfA**-RAs und -Sub-CAs - Überwachung und Einhaltung der Datenschutzbestimmungen - Definition und Überprüfung der Einhaltung der Sicherheitsbestimmungen (insbesondere CPS und Sicherheitskonzept) - Prüfung der Zuordnung von Personen zu Rollen und zu Berechtigungen - Ansprechpartner für sicherheitsrelevante Fragen
Derzeitige Besetzung	Norbert Gust

Tresorverwalter für Tresor 1

Kürzel	TV1
Rollen-Typ	Schließregelung
Mindest-Anzahl Personen	2
Aufgabe der Rolle	Zugriff auf Tresor 1
Verwahrte Objekte	*Alle verwahrten Objekte sind – sofern möglich – versiegelt.* - Notebook mit der virtuellen Maschine der **RfA**-CA - **RfA**-CA Smartcard #1 - PIN für **RfA**-CA Smartcard #4 - Kartenleser für Smartcards - PUK für **RfA**-CA Smartcard #3 - Passwort für Zertifikats-Manager der **RfA**-CA - Passwort für Admin-Konto der **RfA**-CA-VM
Derzeitige Besetzung	Abteilungs- und Gruppenleiter Abt. Infrastruktur zusammen mit einer der leitenden Personen der Competence-Center.

Tresorverwalter für Tresor 2

Kürzel	TV2
Rollen-Typ	Schließregelung
Mindest-Anzahl Personen	2
Aufgabe der Rolle	Zugriff auf Tresor 2
Verwahrte Objekte	*Alle verwahrten Objekte sind – sofern möglich – versiegelt.* - **RfA**-CA Smartcard #2 (Ersatzkarte) - PIN für **RfA**-CA Smartcard #1 - Passwort für lokales Konto des Laptops - PUK für **RfA**-CA Smartcard #4 - Kartenleser für Smartcards
Derzeitige Besetzung	Abteilungs- und Gruppenleiter Abt. Infrastruktur zusammen mit einer der leitenden Personen der Competence-Center.

Tresorverwalter für Tresor 3

Kürzel	TV3
Rollen-Typ	Schließregelung
Mindest-Anzahl Personen	1
Aufgabe der Rolle	Zugriff auf Tresor 3 (DR 1)
Verwahrte Objekte	*Alle verwahrten Objekte sind – sofern möglich – versiegelt.* - **RfA**-CA Smartcard #3 (Ersatzkarte) - PIN für **RfA**-CA Smartcard #2 - PUK für **RfA**-CA Smartcard #1 - Sicherungskopie der **RfA**-CA Datenbank und Log-Dateien von 2015 - Backup der virtuellen Maschine der **RfA**-CA auf optischen Speichermedien - Kopie des Passworts für Zertifikats-Manager der **RfA**-CA - Kopie des Passworts für Admin-Konto der **RfA**-CA-VM - Passwort des Backups von 2023
Derzeitige Besetzung	Justiziariat über ISO (s.o.).

Tresorverwalter für Tresor 4

Kürzel	TV4
Rollen-Typ	Schließregelung
Mindest-Anzahl Personen	2
Aufgabe der Rolle	Zugriff auf Tresor 4 (DR 2)
Verwahrte Objekte	*Alle verwahrten Objekte sind – sofern möglich – versiegelt.* - **RfA**-CA Smartcard #4 (Ersatzkarte) - PIN für **RfA**-CA Smartcard #3 - PUK für **RfA**-CA Smartcard #2 - Sicherungskopien der **RfA**-CA Datenbank und Log-Dateien von 2017 und 2023 - Kopie des Passworts für lokales Konto des Laptops
Derzeitige Besetzung	Abteilungs- und Gruppenleiter Abt. Infrastruktur zusammen mit einer der leitenden Personen der Competence-Center.

5.2.2 Mehraugenprinzip

Ein Vieraugenprinzip ist für das Starten des **RfA**-CA-Dienstes umgesetzt. Es erfolgt kein Key-Recovery von Verschlüsselungsschlüsseln.

5.2.3 Identifizierung und Authentifizierung jeder Rolle

Die Authentifizierung bei den Rollen erfolgt, soweit technisch möglich, über Benutzername und Passwort.

Für die Rollen LA, CCA1, CM, BO und ISO ist das Vier-Augen-Prinzip über aufgetrennte Passwörter und PINs bzw. der Verteilung dieser Objekte auf die Tresore vorgesehen.

5.2.4 Rollentrennung

Zum Öffnen der Tresore sind durch die vorliegenden Schließregelungen mindestens zwei Personen notwendig. Eine Person aus der Gruppe ”Abteilungs- und Gruppenleiter der Abteilung Infrastruktur” darf nicht Mitglied der Gruppe ”Leitende Personen der Competence Center” sein.

Die Rolle eines Tresorverwalters darf zudem nicht in Personalunion mit einer der Rollen LA oder CCA1 übernommen werden. Damit soll die logische Zugriffsberechtigung auf die **RfA**-CA von der physischen Zugriffsberechtigung auf das Notebook mit der **RfA**-CA VM getrennt werden und keine Rolle alleine Zugriff und Zugang zu der eingelagerten **RfA**-CA haben.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

Die CA-Administratoren der **RfA**-CA kennen den Stand der Technik und die Best Practices im Bereich Zertifikatsinfrastruktur. Diese Kenntnisse werden regelmäßig durch z. B. Aufsuchen einer Schulung oder anderer Fortbildungsmaßnahmen aufgefrischt. Alle eingesetzten Personen sind feste Mitarbeiter der RfA.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Eine Sicherheitsüberprüfung der CA-Administratoren der **RfA**-CA ist nicht erforderlich und wurde nicht durchgeführt.

5.3.3 Anforderungen an Schulungen

Die CA-Administratoren der **RfA**-CA sind geeignet qualifiziert (siehe Kapitel 5.3.1). Darüber hinaus werden bei Aufnahme ihrer Tätigkeit als CA-Administratoren keine Anforderungen an bestimmte Schulungen gestellt.

5.3.4 Häufigkeit von Schulungen und Belehrungen

Die CA-Administratoren der **RfA**-CA besuchen alle zwei Jahre eine Zertifikatsinfrastruktur-Schulung oder halten sich auf andere Weise über den Stand der Technik und die Best Practices im Bereich Zertifikatsinfrastruktur auf dem Laufenden.

5.3.5 Häufigkeit und Folge von Job-Rotation

Bei der **RfA**-CA finden keine Job-Rotationen statt.

5.3.6 Maßnahmen bei unerlaubten Handlungen

Die **RfA**-CA Administratoren unterliegen, wie alle Mitarbeiter der RfA, den arbeitsrechtlich zulässigen Sanktionsmöglichkeiten.

5.3.7 Anforderungen an freie Mitarbeiter

Für den Betrieb der **RfA**-CA werden keine freien Mitarbeiter eingesetzt.

5.3.8 Dokumente, die dem Personal zur Verfügung gestellt werden müssen

Die CA-Administratoren der **RfA**-CA erhalten die Mindestanforderungen der Rundfunk-Root-CA und dieses Dokument zur Kenntnis.

5.4 Überwachungsmaßnahmen

5.4.1 Arten von aufgezeichneten Ereignissen

Alle sicherheitsrelevanten Ereignisse der **RfA**-CA werden in der Windows Ereignisanzeige (Ereignisprotokoll) protokolliert. Zu den sicherheitsrelevanten Ereignissen zählen mindestens:

- Start und Beenden der CA
- Änderung der Konfiguration der CA
- Erstellung von Zertifikaten und Sperrlisten
- Erfolgreiche und fehlgeschlagene Zertifikatsanträge

5.4.2 Häufigkeit der Bearbeitung der Aufzeichnungen

Im Fall eines begründeten Verdachts auf Missbrauch der **RfA**-CA wird von den **RfA**-CA Administratoren eine anlassbezogene Auswertung im Rahmen der IT-Sicherheitsverordnung des WDR des

Ereignisprotokolls der **RfA**-CA vorgenommen. Es finden keine darüber hinaus gehenden routinemäßigen Kontrollen des Ereignisprotokolls statt, da die **RfA**-CA offline betrieben wird und damit die meiste Zeit nicht in Betrieb ist. Somit können die Aufzeichnungen nicht automatisiert ausgewertet werden.

5.4.3 Aufbewahrungszeit von Aufzeichnungen

Das Ereignisprotokoll der **RfA**-CA wird während ihrer gesamten Laufzeit auf dem System und in dessen Backup aufbewahrt. Die vorgeschriebene Aufbewahrungszeit von mindestens sieben Tagen wird damit nie unterschritten.

5.4.4 Sicherung der Aufzeichnungen

Das Ereignisprotokoll der **RfA**-CA ist über die Zugriffskontrolle des Betriebssystems gegen unberechtigten Zugriff, Löschung und Manipulation geschützt.

5.4.5 Datensicherung der Aufzeichnungen

Bei der **RfA**-CA wird eine Kopie des Ereignisprotokolls nach jeder Ausstellung oder Sperrung eines Zertifikats sowie nach Ausstellung einer neuen Sperrliste vom CA-Administrator der **RfA**-CA auf einen USB-Speicherstick geschrieben, der sicher in einem der Tresore 3 oder 4 verwahrt wird.

5.4.6 Speicherung der Aufzeichnungen (intern / extern)

Für das Ereignisprotokoll der **RfA**-CA wird kein Überwachungssystem eingesetzt, da die CA offline betrieben wird.

5.4.7 Benachrichtigung der Ereignisauslöser

Da die **RfA**-CA offline betrieben wird und damit die meiste Zeit nicht in Betrieb ist, kann das Ereignisprotokoll nicht automatisiert ausgewertet und nicht über schwerwiegende Ereignisse informiert werden.

5.4.8 Schwachstellenanalyse

Da die **RfA**-CA offline betrieben wird und damit die meiste Zeit nicht in Betrieb ist, findet keine kontinuierliche Schwachstellenanalyse statt. Die Software der **RfA**-CA wird deshalb nur im Bedarfsfall offline gepatcht, da während des gesamten Betriebes keine Internet- oder LAN-Verbindung besteht.

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen

Art und Umfang der Daten, die von der **RfA**-CA aufbewahrt werden:

- Sicherheitskopien des **RfA**-CA Schlüssels auf drei Ersatzkarten
- Passwort-Briefe mit beiden Hälften des lokalen Systemadministrators der **RfA**-CA VM in einem versiegelten Umschlag
- Passwort-Briefe mit beiden Hälften des **RfA**-CA Administrators in einem versiegelten Umschlag
- Passwort-Briefe mit beiden Hälften der PIN für die Smartcards der **RfA**-CA in jeweils einem versiegelten Umschlag
- Passwort-Briefe mit beiden Hälften der PUK für die Smartcards der **RfA**-CA in jeweils einem versiegelten Umschlag
- Sicherungskopie der virtuellen Maschine der **RfA**-CA
- Sicherungskopie der **RfA**-CA Datenbank und Log-Dateien (Ereignisprotokoll)
- Zertifikats- und Sperranträge von **RfA** Sub-CAs an die **RfA**-CA
- Backup der virtuellen Maschine der **RfA**-CA auf einem verschlüsselten Speichermedium

5.5.2 Aufbewahrungsfristen für archivierte Daten

Alle in Abschnitt 5.5.1 genannten Daten werden mindestens während der gesamten Verwendungsdauer des privaten **RfA**-CA Schlüssels aufbewahrt.

5.5.3 Sicherung des Archivs

Die Sicherungskopien sowie die Passwortbriefe werden vor unberechtigtem Zugriff geschützt.

Folgende Informationen sind sicher in einem Tresor verwahrt:

- Zertifikats- und Sperranträge von **RfA** Sub-CAs an die **RfA**-CA
- Passwort für den Zugriff auf die **RfA**-CA
- Ersatz-Smartcards inklusive der zugehörigen PIN/PUK der **RfA**-CA

Folgende Sicherungskopien werden durch Verschlüsselung geschützt und werden in Tresoren verwahrt:

- Sicherungskopie der virtuellen Maschine der **RfA**-CA
- Sicherungskopie der **RfA**-CA Datenbank und Log-Dateien (Ereignisprotokoll)

Auf die Tresore haben nur benannte Tresorverwalter Zugriff und die eingelagerten Objekte sind soweit möglich versiegelt.

5.5.4 Datensicherung des Archivs

Es erfolgt keine gesonderte Sicherung des Archivs. Für die im Tresor aufbewahrten Daten ist keine elektronische Datensicherung erforderlich.

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

Bei der **RfA** bestehen keine Anforderungen zum Zeitstempeln von Aufzeichnungen.

5.5.6 Archivierung (intern / extern)

Für die aufzubewahrenden Daten findet keine elektronische Archivierung in einem speziellen Archivierungssystem statt.

5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen

Für die aufzubewahrenden Daten findet keine elektronische Archivierung in einem speziellen Archivierungssystem statt.

5.6 Schlüsselwechsel der RfA-CA

Der private Schlüssel der **RfA**-CA wird nur so lange zum Ausstellen von **RfA** Sub-CA-Zertifikaten eingesetzt, wie die Gültigkeit der untergeordneten CA-Zertifikate noch innerhalb des Gültigkeitsrahmens des **RfA**-CA-Zertifikats liegt.

Beim Schlüsselwechsel der **RfA**-CA wird neues Schlüsselmaterial generiert, das alte Schlüsselmaterial wird nicht beibehalten.

5.7 Kompromittierung und Geschäftsweiterführung bei der RfA-CA

5.7.1 Behandlung von Vorfällen und Kompromittierungen

Bei Verlust des **RfA**-CA Schlüssels durch Systemausfall oder Löschung der Daten wird der **RfA**-CA Schlüssel aus der Sicherungskopie wiederhergestellt.

Falls im Laufe der Gültigkeitsdauer des **RfA**-CA Zertifikats die verwendeten Kryptoverfahren bzw. Schlüssellängen nicht mehr als hinreichend sicher zu betrachten sind, werden der Informationssicherheitsbeauftragte der **RfA** und die CA-Steuerungsgruppe informiert.

Bei nicht mehr geeignetem Kryptoverfahren, nicht mehr ausreichender Schlüssellänge oder bei Kompromittierung des privaten Schlüssels werden das Zertifikat der **RfA**-CA und alle von ihr aus-

gestellten Sub-CA Zertifikate gesperrt und die **RfA**-CA durch eine neue CA ersetzt. Die Außerbetriebnahme der bestehenden **RfA**-CA ist in Abschnitt 5.8 beschrieben.

Beim Aufbau einer neuen **RfA**-CA wird neues Schlüsselmaterial erzeugt und ein neues Zertifikat bei der Rundfunk-Root-CA beantragt. Anschließend werden alle Sub-CA Zertifikate von der **RfA**-CA neu ausgestellt.

5.7.2 Rechnerressourcen-, Software- und/oder Datenkompromittierung

Vorfälle bei Rechnerressourcen-, Software- und/oder Datenkompromittierung (außer Kompromittierung des privaten Schlüssels) werden unverzüglich behoben.

Bei Defekt der Smartcard mit dem **RfA**-CA Schlüssel oder versehentlicher Löschung der Smartcard wird eine der Ersatzkarten mit der Sicherungskopie des **RfA**-CA Schlüssels verwendet.

Im Fall korrumpierter Software oder Daten d. h. wenn innerhalb der **RfA**-CA fehlerhafte oder manipulierte Rechner, Software und/oder Daten, die Auswirkungen auf die Prozesse der **RfA**-PKI haben, festgestellt werden, muss der Betrieb des entsprechenden IT-Systems unverzüglich eingestellt werden. Das System wird dann unter Wiederherstellung der Software und der Daten aus einer unkompromittierten Datensicherung (System, Datenbank und Ereignisprotokolle) neu aufgesetzt, überprüft und in einem sicheren Zustand in Betrieb genommen. In diesem Fall werden unmittelbar nach der Inbetriebnahme so viele Sperrlisten erstellt, bis die CRLNumber größer ist, als diejenige in der letzten veröffentlichten Sperrliste der **RfA**-CA.

Anschließend wird das fehlerhafte oder modifizierte IT-System analysiert werden. Bei Verdacht einer vorsätzlichen Handlung müssen gegebenenfalls rechtliche Schritte eingeleitet werden.

5.7.3 Verhalten bei Kompromittierung des privaten Schlüssels der RfA-CA

Im Fall eines Verdachts auf Missbrauch der **RfA**-CA wird von den CA-Administratoren unter Einbindung des Informationssicherheitsbeauftragten der **RfA** eine anlassbezogene Auswertung des Ereignisprotokolls der **RfA**-CA vorgenommen.

Bei hinreichendem Verdacht auf eine Kompromittierung des **RfA**-CA Schlüssels wird unverzüglich ein Sperrantrag bei der Rundfunk-Root-CA eingereicht sowie alle von der **RfA**-CA erstellten Sub-CA Zertifikate gesperrt und die **RfA**-CA durch eine neue CA ersetzt. Die Außerbetriebnahme der bestehenden **RfA**-CA ist in Abschnitt 5.8 beschrieben.

Beim Aufbau einer neuen **RfA**-CA wird neues Schlüsselmaterial erzeugt und ein neues Zertifikat bei der Rundfunk-Root-CA beantragt. Anschließend werden alle RfA Sub-CA Zertifikate von der **RfA**-CA neu ausgestellt.

5.7.4 Möglichkeiten zur Geschäftsweiterführung nach einer Kompromittierung

Die Wiederaufnahme des Betriebs nach einem Katastrophenfall entspricht den in den vorangegangen Abschnitten 5.7.1, 5.7.2. und 5.7.3 beschriebenen Vorgehensweisen. Es ist sichergestellt, dass

die Wiederaufnahme des Betriebs nach einem Katastrophenfall ohne Datenverlust (wie zum Beispiel Log-Dateien, Übersicht über ausgestellte und gesperrte Zertifikate) erfolgen kann.

5.8 Schließung einer RfA-CA oder einer Registrierungsstelle

Wenn die **RfA**-CA ihren Betrieb einstellt, stellt sie einen Sperrantrag bei der Rundfunk-Root-CA. Mit der Sperrung des **RfA**-CA Zertifikats werden automatisch auch alle untergeordneten Zertifikate ungültig. Trotzdem sperrt die **RfA**-CA alle von ihr ausgestellten Zertifikate, die noch gültig sind, stellt anschließend eine letzte Sperrliste aus und veröffentlicht diese. Abschließend werden die virtuelle Maschine der **RfA**-CA , die Sicherungskopie der virtuellen Maschine und die Smartcards des **RfA**-CA Schlüssels vernichtet.

6 Technische Sicherheitsmaßnahmen

Die Gewährleistung geeigneter technischer Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb einer Zertifikatsinfrastruktur. Nachfolgend werden die technischen Sicherheitsmaßnahmen beschrieben, die bei der RfA den sicheren Betrieb der **RfA**-CA gewährleisten.

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

Ein Schlüsselpaar der **RfA**-CA wurde unter Zeugen in einer Root-Key-Zeremonie in einer virtuellen Maschine (VM) in Software erzeugt und auf einer produktiven, sowie drei Ersatz-Smartcards hinterlegt. Diese Smartcards sind alle mit einer individuellen PIN geschützt. Anschließend wurden die Schlüssel sicher von der Festplatte gelöscht.

Die RA ist Bestandteil der RfA-CA. Sie verfügt über kein eigenes Schlüsselpaar. Die **RfA**-CA erzeugt keine Schlüssel für ihre Zertifikatsnehmer.

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Da die Schlüssel untergeordneter Zertifizierungsstellen dezentral von der betreffenden **RfA** Sub-CA selbst mit Hilfe des entsprechenden Cryptoproviders der eingesetzten HSM-Module erzeugt werden, ist keine Übermittlung an die **RfA**-CA notwendig.

6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

Die **RfA**-CA übermittelt ihr selbstsigniertes Zertifikat mit dem zu zertifizierenden öffentlichen Schlüssel per E-Mail an die Rundfunk-Root-CA. Durch die Selbst-Signatur des Zertifikats ist sichergestellt, dass die **RfA**-CA im Besitz des zugehörigen privaten Schlüssels ist.

Die CSR (Certificate Signing Request) der **RfA** Sub-CAs werden per HTTPS, per E-Mail oder auf einem Datenträger an die **RfA**-CA übermittelt. Die Zugehörigkeit des CSR zu einem bestimmten Zertifikatantrag wird durch die elektronische Signatur bestätigt.

6.1.4 Lieferung öffentlicher Schlüssel der RfA-CA an Zertifikatsnutzer

Der öffentliche Schlüssel der **RfA**-CA wird von der Rundfunk-Root-CA zertifiziert und an die **RfA**-CA zurückgeliefert. Die **RfA**-CA veröffentlicht ihr **RfA**-CA Zertifikat im AD, LAN, ARD-Netz und im

Internet.

Die URLs, von denen das **RfA**-CA Zertifikat abgerufen werden kann, werden in einer Zertifikatserweiterung in den ausgestellten RfA Sub-CA-Zertifikaten vermerkt (siehe Kapitel 7.1.2).

Der öffentliche Schlüssel einer **RfA** Sub-CA wird von der **RfA**-CA zertifiziert und das Sub-CA-Zertifikat mit dem öffentlichen Schlüssel an die **RfA** Sub-CA zurückgeliefert.

6.1.5 Schlüssellängen

Die **RfA**-CA verwendet das RSA-Verfahren. Das Schlüsselpaar der **RfA**-CA hat eine Schlüssellänge von 4096 Bit.

6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle

Die Schlüssel der **RfA**-CA wurden mittels OpenSSL erzeugt. Das Prüfverfahren und die Anforderungen zur Prüfung des RSA Algorithmus inklusive der Schlüsselgenerierung sind vom NIST spezifiziert.

Die Qualität der erzeugten Public Key Parameter mittels OpenSSL entspricht den Anforderungen aus FIPS 140-2[1]

6.1.7 Schlüsselverwendungen

Das **RfA**-CA Zertifikat enthält eine Schlüsselverwendungs-Erweiterung (`KeyUsage` Erweiterung) mit den Einträgen Zertifikatssignatur und Sperrlistensignatur (`keyCertSign`, `cRLSign`). Die **RfA**-CA verwendet ihren zu diesem Zertifikat zugehörigen privaten Schlüssel nur zur Unterzeichnung von Zertifikaten und Sperrlisten. Zertifikatsprüfer (Relying Parties) müssen diese Schlüsselverwendungszwecke prüfen, bevor sie das Zertifikat verwenden.

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

Der private Schlüssel der **RfA**-CA wird in einer Smartcard gespeichert und genutzt, die nach Common Criteria EAL4+ zertifiziert ist.

6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m)

Die Aktivierung des privaten Schlüssels der **RfA**-CA wird nach dem Vier-Augen-Prinzip geschützt.

[1] siehe https://www.openssl.org/docs/fips/fipsvalidation.html

6.2.3 Hinterlegung privater Schlüssel

Der private Schlüssel der **RfA**-CA wird nicht bei einer anderen Instanz hinterlegt, d. h. es findet kein Key Escrow statt. Die **RfA**-CA bietet für die **RfA** Sub-CAs keinen Schlüsselhinterlegungsdienst an.

6.2.4 Sicherung privater Schlüssel

Bei der **RfA**-CA Root-Key-Zeremonie wurde von dem privaten Schlüssel unter Zeugen in drei Ersatzkarten importiert. Als Ersatzkarten wurde der gleiche Typ Smartcard wie für die produktive Smartcard verwendet, der nach Common Criteria EAL4+ zertifiziert ist. Jede Smartcard ist mit einer individuellen PIN versehen. Die Ersatz-Smartcards werden in einem anderen Tresor als die produktive Smartcard aufbewahrt.

6.2.5 Archivierung privater Schlüssel

Die Archivierung privater Schlüssel sowie deren Zugriffsschutz erfolgt wie unter Abschnitt 6.2.4 beschrieben.

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Das Schlüsselmaterial der **RfA**-CA befindet sich ausschließlich auf den verwendeten Smartcards.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Die Schlüssel der **RfA**-CA wurden auf Smartcards gespeichert (siehe Kapitel 6.1.1).

6.2.8 Aktivierung privater Schlüssel

Der private Schlüssel der **RfA**-CA wird erst durch die Eingabe der zugehörigen PIN im Vier-Augen-Prinzip aktiviert.

6.2.9 Deaktivierung privater Schlüssel

Der private Schlüssel der **RfA**-CA kann durch Beendigung des Zertifikatsdienstes, Herunterfahren des Systems oder Entfernen der Smartcard aus dem zugehörigen Leser deaktiviert werden.

6.2.10 Zerstörung privater Schlüssel

Um den privaten Schlüssel der **RfA**-CA zu vernichten, werden die Smartcards physisch zerstört (geschreddert). Zusätzlich wird die gesamte VM mit einem geeigneten Lösch-Tool sicher gelöscht.

6.2.11 Beurteilung kryptographischer Module

Die verwendeten Smartcards sind nach Common Criteria EAL4+ zertifiziert (siehe Kapitel 6.2.1).

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Der öffentliche Schlüssel der **RfA**-CA wird in der CA-Datenbank auf dem CA-Server gespeichert. Eine darüber hinausgehende Archivierung des öffentlichen Schlüssels erfolgt durch das Backup der CA-Datenbank.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Das von der Rundfunk-Root-CA ausgestellte **RfA**-CA Zertifikat ist ab dem Ausstellungszeitpunkt 20 Jahre gültig. Die von der **RfA**-CA ausgestellten **RfA** Sub-CA Zertifikate sind zehn Jahre gültig.

Der private Schlüssel der **RfA**-CA wird nur für zehn Jahre zur Ausstellung von **RfA** Sub-CA Zertifikaten genutzt. In den letzten zehn Jahren seiner Laufzeit wird er nicht mehr zur Ausstellung weiterer Sub-CA Zertifikate genutzt, da die **RfA** Sub-CA Zertifikate ab diesem Zeitpunkt keine zehn Jahre mehr gültig sein können.

6.4 Aktivierungsdaten

6.4.1 Aktivierungsdaten

Das Passwort zur Anmeldung an der **RfA**-CA ist zweigeteilt in zweimal mindestens sechs Zeichen, insgesamt mindestens zwölf Zeichen, lang. Die beiden Passworthälften wurden unter Berücksichtigung der diesbezüglichen Vorgaben der **RfA** Passwort Policy von den beiden **RfA**-CA Administratoren während der Root-Key-Zeremonie festgelegt, niedergeschrieben und in je einem Umschlag versiegelt sowie in ihrem persönlichen lokalen Password-Safe gespeichert.

Zusätzlich ist die PIN zur Aktivierung des privaten Schlüssels der **RfA**-CA vier Zeichen lang. Sie wurde von den beiden **RfA**-CA Administratoren während der Root-Key-Zeremonie der **RfA**-CA festgelegt.

6.4.2 Schutz von Aktivierungsdaten

Die beiden Passworthälften zur Anmeldung an der **RfA**-CA und die beiden PIN-Hälften zur Entsperrung der SmartCard sind nur den Administratoren der **RfA**-CA bekannt. Die beiden Passworthälften werden niemals einem Administrator in seiner Funktion als **RfA**-CA Administrator bekannt gegeben und voneinander getrennt aufbewahrt, so dass das Vier-Augen-Prinzip stets gewahrt bleibt.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Bei der **RfA**-CA handelt es sich um eine virtuelle Maschine (VMware Workstation) mit dem Betriebssystem Windows Server 2012 R2, die als Offline-CA auf einem Notebook im Stand-Alone Modus betrieben wird. Das in der VM eingesetzte Windows 7 Betriebssystem wird entsprechend den hierfür gültigen Vorgaben der **RfA** installiert. Das Host- und das Gastbetriebssystem in der VM verfügt über keine Netzwerkanbindung und ist keinem AD angeschlossen. Bei Nicht-Gebrauch wird es heruntergefahren und kann nur nach manueller Eingabe der zugehörigen Passwörter wieder gestartet werden. Bei Nicht-Gebrauch wird das Notebook im Tresor 1 bei der **RfA** aufbewahrt.

Die **RfA**-CA wird durch geeignete Benutzerauthentisierung und Zugriffskontrolle auf Betriebssystem-Ebene vor unberechtigten Zugriffen geschützt. Sowohl der lokale Systemadministrator als auch der **RfA**-CA Administrator haben ein Passwort bestehend aus mindestens 12 Zeichen. Weitere Benutzer haben keinen Zugriff auf die VM.

6.5.2 Beurteilung von Computersicherheit

Für die **RfA**-CA gibt es keine Gütesiegel in Form von Produktzertifikaten wie bspw. eine CC-Evaluierung und Bestätigung.

Die verwendeten Smartcards sind nach Common Criteria EAL4+ zertifiziert.

6.6 Technische Maßnahmen während des Life Cycles

6.6.1 6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

Es findet keine Software-Entwicklung statt.

6.6.2 6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Da die **RfA**-CA als Offline-CA die meiste Zeit nicht in Betrieb ist und niemals Netzzugang hat, werden keine aktuellen Updates und Patches für die Systeme der **RfA**-CA eingespielt.

6.6.3 Sicherheitsmaßnahmen während der Life Cycles

Da die **RfA**-CA offline betrieben wird und für die **RfA**-CA weder Sicherheitsmaßnahmen bei der Entwicklung noch beim Computermanagement notwendig sind, gibt es für die virtuelle Maschine der **RfA**-CA folglich auch keine Überprüfung und Bewertung während des Lebenszyklus der RfA-CA, ob und in welchem Maße Sicherheitsmaßnahmen korrekt umgesetzt sind und ob sie wie beabsichtigt betrieben werden.

6.7 Sicherheitsmaßnahmen für Netze

Die **RfA**-CA wird auf einer offline Betriebssysteminstanz betrieben, daher gibt es für die **RfA**-CA keine weiteren Sicherheitsmaßnahmen für Netze.

6.8 Zeitstempel

Bei der RfA wird kein Zeitstempeldienst betrieben.

7 Profile von Zertifikaten, Sperrlisten und OCSP

7.1 Zertifikatsprofile

7.1.1 Versionsnummern

Die **RfA**-CA setzt die Versionsnummer in den ausgestellten **RfA** Sub-CA Zertifikaten auf den Wert 2 (Version 3), d.h. sie stellt X.509v3 Zertifikate aus.

7.1.2 Zertifikatserweiterungen

Die **RfA**-CA fügt mindestens folgende Zertifikatserweiterungen zu den RfA Sub-CA Zertifikaten hinzu:

- BasicConstraints (Basiseinschränkungen)
- KeyUsage (Schlüsselverwendung)
- CRLDistributionPoints (Sperrlisten-Verteilungspunkte)
- AuthorityKeyIdentifier (Stellenschlüsselkennung)
- SubjectKeyIdentifier (Schlüsselkennung des Antragstellers)
- CertificatePolicies (Anwendbare CPs, für Sub-CA-Zertifikate, die ab dem 01.02.2022 ausgestellt wurden)

Die Erweiterungen `BasicConstraints` und KeyUsage werden als kritisch, alle anderen als nichtkritisch markiert.

7.1.3 Algorithmen OIDs

Es wird der Signaturalgorithmus „sha256WithRSAEncryption“ verwendet. Als Algorithmen-Identifier für den Subject Public Key (Teilnehmerschlüssel) in CA-Zertifikaten wird bis auf weiteres der folgende genutzt: • rsaEncryption (OID: 2.840.113549.1.1.1)

7.1.4 Namensformate

Siehe Abschnitt 3.1.4

7.1.5 Namensbeschränkungen

Bei der **RfA**-CA gibt es keine Namensbeschränkungen. Die Interpretation der Namen erfolgt wie in Abschnitt 3.1.4 beschrieben.

7.1.6 OIDs der Zertifikatsrichtlinien

Die **RfA**-CA verwendet in den von ihr ausgestellten **RfA** Sub-CA Zertifikaten die Certificate Policies Erweiterung mit einer Objektkennung (Object Identifier - OID) unterhalb des OID-Präfixes der Rundfunk-Root-CA (1.3.6.1.4.1.42638) als Referenz auf dieses Policy-Dokument.

Die Anforderung nach RfA-übergreifender Kennzeichnung von WLAN-Zertifikaten und weConnect betrifft die **RfA**-CA nicht, da sie keine WLAN-Clientzertifikate ausstellt. Sie gibt diese Anforderung jedoch für die **RfA** Sub-CAs in der für diese gültigen Zertifizierungsrichtlinie (CP) verbindlich vor.

7.1.7 Nutzung der Erweiterung ”Policy Constraints”

Es werden keine Beschränkungen für Sicherheitsrichtlinien (Policy Constraints) in den ausgestellten **RfA** Sub-CA Zertifikaten verwendet.

7.1.8 Syntax und Semantik von ”Policy Qualifiers”

Die **RfA**-CA verwendet in den von ihr ausgestellten **RfA** Sub-CA Zertifikaten keine CertificatePolices Erweiterung und damit auch keine Policy Qualifier, die Bestandteil der CertificatePolices Erweiterung sind.

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung Zertifikatsrichtlinie

Gemäß Abschnitt 7.1.2 ist eine CertificatePolices Erweiterung (Erweiterung Zertifikatsrichtlinie) in allen Zertifikaten der gesamten Rundfunk-PKI immer als unkritisch gekennzeichnet.

7.2 Sperrlistenprofile

7.2.1 Versionsnummer(n)

Die **RfA**-CA setzt die Versionsnummer in ihrer Sperrliste auf Version 2 (=Wert 1), d. h. sie stellt X.509v2 Sperrlisten aus.

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

Die **RfA**-CA fügt mindestens folgende Erweiterungen zu ihrer Sperrliste hinzu:

- AuthorityKeyIdentifier (Stellenschlüsselkennung)
- CRLNumber (Sperrlistennummer)
- NextCRLPublish (Nächste Sperrlistenveröffentlichung)
- PublishedCRLLocations (Veröffentlichte Sperrlistenstandorte)

Diese Sperrlistenerweiterungen sind alle als nicht kritisch markiert. Die **RfA**-CA verwendet keine kritischen Erweiterungen in ihren Sperrlisten.

7.3 Profile des Statusabfragedienstes (OCSP)

7.3.1 Versionsnummer(n)

Die **RfA**-CA bietet keinen Statusabfragedienst (OCSP) an.

7.3.2 OCSP Erweiterungen

Die **RfA**-CA bietet keinen Statusabfragedienst (OCSP) an.

8 Überprüfungen und andere Bewertungen

Audits der Rundfunk-Root-CA und der **RfA**-CAs werden von der ARGE Rundfunk-Betriebstechnik (RBT) durchgeführt. Dabei soll die regelgerechte Implementierung mit Schwerpunkt auf zertifikatsspezifische Themen, wie z. B. Prüfung der Prozesse und Aufgaben der Admins, bei allen Mitgliedern überprüft werden. Es werden sowohl das CPS-Dokument auf Einhaltung der Mindestanforderungen als auch die technische Implementierung geprüft. Als Grundlage dient der „Prüfkatalog der Rundfunk-Root-CA zur Konformitätsprüfung von teilnehmenden RfA-CAs“. Das Ergebnis wird in einem Bericht zusammengefasst, dieser enthält auch eine Empfehlung für mögliche Nachprüfungen.

Wurden im Rahmen der Prüfung Mängel festgestellt, muss das CA-Steuerungsmitglied der **RfA** die Prüfungsergebnisse zusammen mit den CA-Ansprechpartnern gemeinsam bewerten und über das weitere Vorgehen entscheiden. Die festgestellten Mängel müssen priorisiert und geeignete Korrekturmaßnahmen prioritätengesteuert eingeleitet und koordiniert werden. Das Vorgehen und die Behebung müssen dem Betreiber 3 Monate nach Zugang des Berichts gemeldet werden. Bei sicherheitskritischen Feststellungen muss eine vorgezogene Nachprüfung stattfinden. Die Kosten hierzu sind über die RBT Umlage von dem jeweiligen Teilnehmer zu tragen.

Bei Neuaufnahme eines Mitglieds soll diese Überprüfung initial spätestens drei Monate nach der Aufnahme durchgeführt werden. Bei Bestandmitgliedern wählt der Betreiber mit geeignetem zeitlichen Vorlauf vor Erstellung des Jahresberichts mindestens zwei (innerhalb von drei Jahren, sollen alle Teilnehmer einmal geprüft worden sein) Mitglieder der Rundfunk-CA zufällig aus und unterzieht diese einer gesonderten Prüfung.

Die Ergebnisse dieser Überprüfung finden Eingang in den Jahresbericht. Daneben finden ggf. interne Überprüfungen der **RfA**-CA nach den Maßgaben der folgenden Abschnitte statt.

8.1 Häufigkeit und Bedingungen für Überprüfungen

Im Fall eines begründeten Verdachts auf Missbrauch der **RfA**-CA wird von den CA- Administratoren der **RfA**-CA unter Einbindung des Informationssicherheitsbeauftragten eine anlassbezogene Auswertung der Log-Daten der **RfA**-CA vorgenommen. Es finden keine darüber hinaus gehenden routinemäßigen Kontrollen der Log-Daten statt, da die **RfA**-CA offline betrieben wird und damit die meiste Zeit nicht in Betrieb ist. Somit können die Log-Daten nicht automatisiert ausgewertet werden.

Zusätzlich werden jährlich durch interne Audits die aufgezeichneten System- und Anwendungsereignisse sowie die Prozesse der **RfA**-CA stichprobenhaft überprüft.

8.2 Identität/Qualifikation des Prüfers

Der Prüfer verfügt über eine geeignete Qualifikation als Auditor.

8.3 Stellung des Prüfers zum Bewertungsgegenstand

Der Prüfer gehört weder zu der überprüften Abteilung noch ist er dieser Abteilung unterstellt.

8.4 Durch Überprüfungen abgedeckte Themen

Bei der Konformitätsprüfung der **RfA**-CA werden mindestens folgende Bereiche stichprobenhaft untersucht:

- Prozesse des Zertifikatsmanagements
- Physikalische Sicherheitsmaßnahmen
- Technische Sicherheitsmaßnahmen
- Organisatorische Sicherheitsmaßnahmen
- Personelle Sicherheitsmaßnahmen

8.5 Reaktionen auf Unzulänglichkeiten

Werden im Rahmen der Prüfung Mängel festgestellt, wird der IT-Sicherheitsbeauftragte der **RfA** die Prüfungsergebnisse mit den Administratoren der **RfA**-CA gemeinsam bewerten und über das weitere Vorgehen entscheiden. Die festgestellten Mängel werden priorisiert und geeignete Korrekturmaßnahmen prioritätengesteuert eingeleitet und koordiniert.

8.6 Information über Bewertungsergebnisse

Die Ergebnisse des Audits werden dem Betreiber der Rundfunk-Root-CA zur Verfügung gestellt. Dieser fasst die Ergebnisse zusammen und stellt sie der CA-Steuerungsgruppe im Rahmen eines jährlichen Berichts zur Verfügung.

9 Andere finanzielle und rechtliche Angelegenheiten

9.1 Preise

Für die Nutzung der **RfA**-PKI werden keine Gebühren erhoben.

9.2 Finanzielle Zuständigkeiten

Finanzielle Aspekte werden in diesem Dokument nicht beschrieben.

9.3 Vertraulichkeitsgrad von Geschäftsdaten

9.3.1 Definition von vertraulichen Informationen

Jegliche Informationen über Teilnehmer und Antragsteller, die nicht unter den nächsten Abschnitt fallen, werden als vertrauliche Informationen eingestuft und behandelt.

9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören

Alle Informationen, die in den herausgegebenen Zertifikaten und Sperrlisten explizit (z. B. E-Mail Adresse) oder implizit (z. B. Daten über die Zertifizierung) enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft. Hierzu zählt z. B. der Name und Betreiber einer **RfA** Sub-CA.

9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen

Der Betreiber der **RfA**-CA trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen. Daten werden im **RfA**-Rahmen der Diensterbringung nur weitergegeben, wenn zuvor eine Vertraulichkeitserklärung unterzeichnet wurde. Die mit den Aufgaben betrauten Mitarbeiter wurden auf Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet.

9.4 Datenschutz von Personendaten

9.4.1 Datenschutzkonzept

Die zur Leistungserbringung erforderliche elektronische Speicherung und Verarbeitung von personenbezogenen Daten erfolgt in Übereinstimmung mit der DSGVO und dem im Staatsvertrag angegebenen Datenschutzgesetz.

9.4.2 Als persönlich behandelte Daten

Für personenbezogene Daten gelten die Regelungen für den Betrieb der **RfA**-CA aus Abschnitt 9.3.1 analog.

9.4.3 Daten, die nicht als persönlich behandelt werden

Für personenbezogene Daten gelten die Regelungen für den Betrieb der **RfA**-CA aus Abschnitt 9.3.2 analog.

9.4.4 Zuständigkeiten für den Datenschutz

Für personenbezogene Daten gelten die Regelungen für den Betrieb der **RfA**-CA aus Abschnitt 9.3.3 analog.

9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten

Die **RfA**-CA holt die Zustimmung einer jeden **RfA** Sub-CA als Zertifikatsnehmer ein, dass sie der Nutzung von personenbezogenen Daten durch die **RfA**-CA zustimmt, soweit dies zur Leistungserbringung erforderlich ist. Sie veröffentlicht nur Informationen, die als nicht vertraulich behandelt werden (siehe Abschnitt 9.4.3) und deren Veröffentlichung nicht widersprochen wurde.

9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften

Die RfA-CAs unterliegen dem Recht der Bundesrepublik Deutschland. Sie geben vertrauliche und personenbezogene Informationen an staatliche Organe in Übereinstimmung mit den geltenden Gesetzen nur dann weiter, wenn entsprechende Entscheidungen vorliegen. Die Entscheidungen erfolgt durch bzw. nach Abstimmung mit der Juristischen Direktion und dem Informationssicherheitsbeauftragten der **RfA**.

9.4.7 Andere Bedingungen für Auskünfte

Es gibt keine anderen Bedingungen für Auskünfte.

9.5 Geistiges Eigentumsrecht

Der Betreiber der **RfA**-CA hat das alleinige Nutzungsrecht an dem vorliegenden Dokument. Eine Weitergabe von veränderten Fassungen dieses Dokuments ist ohne Zustimmung von dem Betreiber der **RfA**-CA nicht zulässig.

9.6 Zusicherungen und Garantien

9.6.1 Zusicherungen und Garantien der CA

Die **RfA**-CA verpflichtet sich, die Mindestanforderungen der Rundfunk-Root-CA und alle im Rahmen dieser CPS beschriebenen Aufgaben geeignet umzusetzen und ihre Aufgaben nach bestem Wissen und Gewissen durchzuführen.

9.6.2 Zusicherungen und Garantien der RA

Die Registrierungsstelle ist Bestandteil der **RfA**-CA. Ihre Zusicherung erfolgt gemäß Kapitel 9.6.1.

9.6.3 Zusicherungen und Garantien der Zertifikatsnehmer

Es gelten die Regelungen für den Betrieb der **RfA**-CA aus Abschnitt 4.5.1.

9.6.4 Zusicherungen und Garantien der Zertifikatsnutzer

Es gelten die Regelungen für den Betrieb der **RfA**-CA aus den Abschnitten 4.5.2, 4.9.6 und 6.1.7.

9.6.5 Zusicherungen und Garantien anderer Zertifikatsinfrastruktur-Teilnehmer

Sofern weitere Teilnehmer als Dienstleister in den Zertifizierungsprozess eingebunden werden, ist der beauftragte Dienstleister zur Einhaltung der Mindestanforderungen der Rundfunk-Root-CA und dieser CPS verpflichtet.

9.7 Haftungsausschlüsse

Haftungsausschlüsse sind bei der **RfA**-CA nicht geregelt.

9.8 Haftungsbeschränkungen

Haftungsbeschränkungen sind bei der **RfA**-CA nicht geregelt.

9.9 Schadensersatz

Bei der **RfA**-CA gibt es keine Regelungen zum Schadensersatz.

9.10 Gültigkeitsdauer und Beendigung

9.10.1 Gültigkeitsdauer

Dieses Policy-Dokument tritt nach Veröffentlichung in Kraft.

9.10.2 Beendigung

Dieses Dokument ist solange gültig, bis es durch eine neue Version ersetzt wird oder der Betrieb der **RfA**-CA eingestellt wird.

9.10.3 Auswirkung der Beendigung und Weiterbestehen

Von einer Aufhebung dieses Policy-Dokuments unberührt bleibt die Verantwortung zum Schutz vertraulicher Informationen und personenbezogener Daten.

9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern

Individuellen Mitteilungen und Absprachen mit Teilnehmern sind bei der **RfA**-CA nicht geregelt und bleiben den CAs freigestellt.

9.12 Ergänzungen

9.12.1 Verfahren für Ergänzungen

Eine Änderung dieses Policy-Dokuments kann nur durch den Zuständigen für dieses Dokument erfolgen (siehe Abschnitt 1.5.1).

9.12.2 Benachrichtigungsmechanismen und –fristen

Bei Änderung von Anforderungen in diesem Policy-Dokument – bspw. aufgrund von geänderten Mindestanforderungen der Rundfunk-Root-CA – werden die RfA Sub-CAs innerhalb eines Monats informiert.

9.12.3 Bedingungen für OID Änderungen

OIDs werden für die Identifikation von Zertifikatsrichtlinien bei der RfA sind wie folgt aufgebaut:

- 1.3.6.1.4.1.42638.1.7 RfA-CA
- 1.3.6.1.4.1.42638.1.7.1 Certificate Policy (CP) Dokument der RfA-CA
- 1.3.6.1.4.1.42638.1.7.1.<n> Hauptversionsnummer CP
- 1.3.6.1.4.1.42638.1.7.1.<n>.<m> Nebenversionsnummer CP
- 1.3.6.1.4.1.42638.1.7.2 Certification Practice Statements (CPS) Dokument der RfA-CA
- 1.3.6.1.4.1.42638.1.7.2.<n> Hauptversionsnummer CPS
- 1.3.6.1.4.1.42638.1.7.2.<n>.<m> Nebenversionsnummer CPS
- 1.3.6.1.4.1.42638.1.7.3 RfA Sub-CA 01 Certification Practice Statements (CPS)
- 1.3.6.1.4.1.42638.1.7.3.<n> Hauptversionsnummer Sub-CA 01 CPS
- 1.3.6.1.4.1.42638.1.7.3.<n>.<m> Nebenversionsnummer Sub-CA 01 CPS
- 1.3.6.1.4.1.42638.1.7.4 RfA Sub-CA 11 Certification Practice Statements (CPS)
- 1.3.6.1.4.1.42638.1.7.5 RfA Sub-CA 12 Certification Practice Statements (CPS)

Wenn Änderungen in diesem Policy-Dokument vorgenommen werden, die sicherheitsrelevante oder andere substanzielle Aspekte betreffen oder aus anderen Gründen eine Änderung der Versionsnummer des Dokuments erfordern, ist eine entsprechende Anpassung der OID dieses Dokuments an die geänderte Versionsnummer erforderlich.

Die OID zur Identifikation des Policy-Dokuments der **RfA**-CA ist nicht in einer Certificate Polices Erweiterung der ausgestellten Zertifikate für RfA Sub-CAs enthalten.

9.13 Verfahren zur Schlichtung von Streitfällen

Verfahren zur Schlichtung von Streitfällen ist bei der **RfA**-CA nicht geregelt. Grundsätzlich sind die in Abschnitt 1.5.2 genannten Stellen für die Konfliktbeilegung zuständig.

9.14 Zugrundeliegendes Recht

Der Betrieb der **RfA**-CA unterliegt den Gesetzen der Bundesrepublik Deutschland.

9.15 Einhaltung geltenden Rechts

Eine **RfA**-CA ist kein Zertifizierungsdienstanbieter im Sinne des deutschen Signaturgesetzes und stellt keine qualifizierten Zertifikate aus. Es werden allenfalls Zertifikate ausgestellt, mit denen fortgeschrittene elektronische Signaturen gemäß dem deutschen Signaturgesetz erzeugt werden können.

9.16 Sonstige Bestimmungen

9.16.1 Vollständigkeitserklärung

Die Ausgabe einer neuen Version dieser Mindestanforderungen ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2 Abgrenzungen

Keine

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser CPS unwirksam sein, 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 weitgehend entspricht. Im Falle von Lücken gilt ebenfalls dasjenige als vereinbart, was nach Sinn und Zweck dieser CPS vernünftigerweise vereinbart worden wäre, hätte man die Angelegenheit von vorn herein bedacht.

9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

Rechtliche Auseinandersetzungen, die aus dem Betrieb einer **RfA**-CA herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland. Erfüllungsort und ausschließlicher Gerichtsstand ist Köln als Sitz des Betreibers der **RfA**-CA.

9.16.5 Höhere Gewalt

Es gibt bei der **RfA**-CA keine Regelungen zu höherer Gewalt.

9.16.6 Andere Bestimmungen

Es gibt keine weiteren Bestimmungen.