NDR

Regelungen für den Zertifizierungsbetrieb (CPS) der NDR-CA-2020

Inhaltsverzeichnis

1 Einleitung

In diesem Dokument wird **RfA** (fettgedruckt) als Synonym für den **NDR** verwendet.

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.

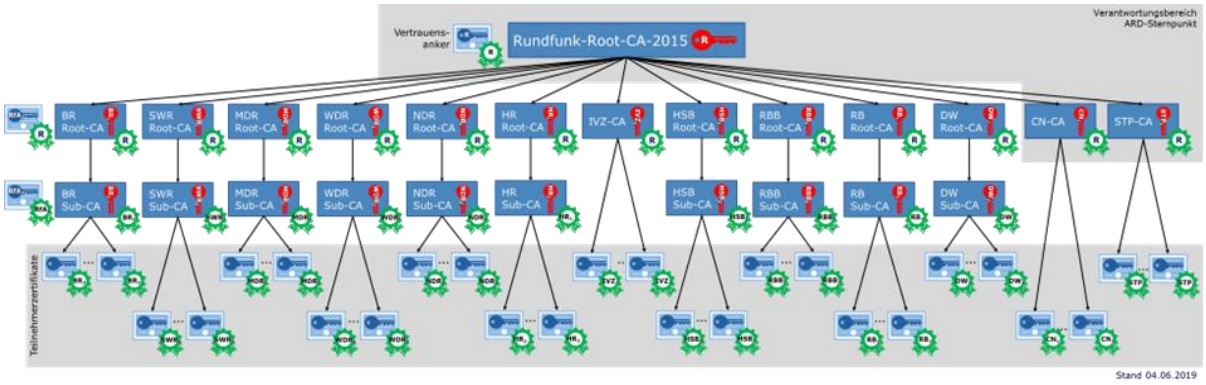

Abbildung 1: Beispielhafter Überblick über die Struktur der gesamten Zertifikatsinfrastruktur des ARD-Netzes

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.

Kurzbeschreibung der Lösung:

Die **RfA**-CA wird domänen-integriert in einer Virtuellen Maschine (VM) betrieben. Das Schlüsselmaterial der **RfA**-CA wird auf zwei redundant betriebenen Hardware Security Modules (HSM) gespeichert. Bei Nichtgebrauch ist die **Rfa**-CA mitsamt des Zertifizierungsdienstes heruntergefahren und die verbundenen Schlüsselpartitionen der HSMs werden von der

Zertifizierungsstelle getrennt. Die auf den HSMs befindlichen Schlüsselpartitionen können nur verbunden werden, indem im Vier-Augen Prinzip ein zweigeteiltes Partitionspasswort eingegeben wird.

1.2 Name und Kennzeichnung des Dokuments

Name:	Regelungen für den Zertifizierungsbetrieb (CPS) der Offline **RfA**-CA-2020
Version:	3.4
Datum:	10.01.2024
OID:	keine

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-CA / **RfA**-System-CA und **RfA**-User-CA von den gleichen Personen bei der **RfA** betrieben werden, ist keine gesonderte Identitätsprüfung bei der Registrierung der **RfA**-Issuing-CA / **RfA**-System-CA und **RfA**-User-CA 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 Andere Teilnehmer

CA-Steuerungsgruppe

Die **RfA**-CA ist mit einem Sitz in der CA-Steuerungsgruppe vertreten. Die RfA hat **Dr. Dirk Höhne** (d.hoehne@ndr.de) als Vertreter in der CA-Steuerungsgruppe benannt.

CA-Ansprechpartner

Die **RfA** hat dem Betreiber der Rundfunk-Root-CA **Andreas Fischer** (a.fischer@ndr.de) als CA-Ansprechpartner und **Lars Lucas** (l.lucas@ndr.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: **http(s)://ca-info.ndr.de**

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen 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 Verwendungen 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 ist **Herr Andreas Fischer** 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: **http(s)://ca-info.ndr.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
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	**Certification 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
CP	**Certificate Policy** Zertifizierungsrichtlinie
CPS	**Certification Practice Statement** Regelungen für den Zertifizierungsbetrieb
CSR	**CertificateSigningRequest** Zertifikatsantrag
CSR	**CertificateSigningRequest** Zertifikatsantrag
DN	**Distinguished Name Vollqualifizierter Name** Vollqualifizierter Name
DNS	**Domain Name System** Namensauflösung im Internet
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 Infrastructure** Infrastruktur für X.509 Zertifikate
PIN	**Personal Identification Number** Persönliche Identifikationsnummer
RADIUS	**Remote Authentication Dial-In User Service** Netzwerkprotokoll zur Authentifizierung
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
UPN	**User Principal Name** Eindeutiges Benamungsschema von Benutzer- und Computerobjekten im AD
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 einen Web-Application-Proxy im Internet zur Verfügung gestellt. 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 Zugriffskontrollen 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 aussagefähige 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=**NDR**-CA-2020, O=**NDR**, C=DE

Statt der Rundfunkanstalt kann hier auch die Gemeinschaftseinrichtung oder Dritte [1] stehen!

[1] Dritte sind Teilnehmer des ARD-Netzes gemäß Verfahren zur Anbindung Dritter an das ARD-CN

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 des privaten Schlüssels

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 durch Bereiche der **Hauptabteilung Informations-, Medien- und Verbreitungstechnik** beantragt werden. Die Berechtigung wird anhand der Organisationsstruktur der **NDR-Produktionsdirektion** überprüft.

3.2.6 Kriterien zur 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. Ein Sub-CA-Zertifikat darf nur durch die Abteilungsleitung der **Abteilung Infrastruktur** beantragt werden.

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 des 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 Signatur 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 Names der **RfA** Sub-CA im Feld Subject.
- Die Schlüssellänge muss mindestens 4096 Bits sein (RSA-Verfahren).

- 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 aktivierenn die VM mit der Offline CA. Die erforderlichen Passworthälften für den Betrieb der **RfA**-CA sind in den persönlichen, lokalen Password-Safes der beiden CA-Administratoren hinterlegt.

Die Ausstellung und Ausgabe von **RfA** Sub-CA Zertifikaten erfolgt nur für angenommene, gültige und gemäß 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 Kapitel 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 der Prüfung des Zertifikatsantrages (siehe Kapitel 4.2) wird das Zertifikat auf der **RfA**-CA durch einen **Zertifikatsmanager** der **RfA**-CA ausgestellt.

Da das Zertifikat keine privaten Schlüssel oder andere vertrauliche Daten enthält, wird es dem Antragsteller auf einem elektronischen Wege bereitgestellt.

Der ausführende CA-Administrator der **RfA**-CA fertigt eine schriftliche Protokollnotiz [1] über den Vorgang an, die von beiden CA-Administratoren unterschrieben wird. Diese Protokollnotitz wird elektronisch archiviert.

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 in einem Tresor in der **RfA** verwahrt.

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

Nach der Zertifikatausstellung wird das ausgestellte Zertifikat dem Zertifikatnehmer in geeigneter Weise (siehe Kapitel 4.3.1) durch die CA übermittelt oder der Zertifikatnehmer über dessen Ausstellung informiert.

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 wird niemals außerhalb der sicheren Grenzen des HSM im Klartext abgespeichert oder in anderer Weise zugänglich gemacht.

> **Beschreibung:**Bereits bei Installation der RfA-CA wird der private Schlüssel der Zertifizierungsstelle durch einen hersteller-eigenen, sogenannten „Crypto Provider“ in einem redundant ausgelegten HSM Partitionsverbund angelegt. Die direkte Generierung von Schlüsselmaterial auf HSM Partitionen schließt eine Kompromittierung oder Manipulation während des Generierungsvorgangs aus und stellt sicher, dass Schlüsselmaterial das HSM-eigene Ökosystem nicht verlassen kann. Die im HSM angelegten Partitionen sind grundsätzlich logisch getrennt von anderen Partitionen und werden im Vorfeld durch einen HSM Administrator angelegt. Die spätere Initialisierung der Partitionen wird dabei vom CA Administrator durchgeführt und geht mit einer Passwort-Vergabe einher, welche durch ein Vier-Augen-Prinzip überwacht und aufgeteilt wird. Die Passwort-Vergabe sowie dessen Verwaltung erfolgt hierbei autark vom HSM Administrator. Somit wird sichergestellt, dass ein HSM Administrator zu keiner Zeit einen Signaturvorgang oder anderweitigen Zugriff auf die HSM-Partition erhält. Kryptografisch wird weiterhin jede einzelne Partition durch einen HSM-internen Schlüssel geschützt. Der Betrieb einer HSM Appliance ist so ausgelegt, dass

kryptographische Befehle vollständig isoliert vom Betriebssystem des HSM ausgeführt werden und so ein nicht autorisierter Zugriff außerhalb des angeschlossenen Client-Systems nicht möglich ist. Physikalische Maßnahmen wie eine Erkennung der Gehäuse-Unversehrtheit oder Messung von elektrischen Strömen stellen sicher, dass Manipulationen der Hardware jederzeit erkannt werden können. Sofern eine dieser Manipulationen erkannt werden, wird das HSM-interne Schlüsselmaterial der Partition unwiderruflich gelöscht und somit eine weitere Partitionsverwendung unterbunden. Alle beschriebenen Sicherheitsmaßnahmen gelten ebenfalls für HSM Backup Systeme, da diese mit den gleichen Maßnahmen und Funktionalitäten einer HSM Appliance ausgestattet sind. Ein Export von Schlüsselmaterial aus dem HSM Ökosystem ist nicht möglich.

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. Die **RfA** Sub-CAs sind für die Sicherung ihrer privaten Schlüssel selbst verantwortlich, so dass sie diese im Notfall wiederherstellen können.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch 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 Schlüsselpaars (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 Zertifikat 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 ZertifikatsinfrastrukturTeilnehmer 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 für 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 für 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 für Schlüsselerneuerungen durch die CA

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

4.7.7 Benachrichtigung anderer ZertifikatsinfrastrukturTeilnehmer 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

Die 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 anderer ZertifikatsinfrastrukturTeilnehmer 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 gültig sind.
- Der private Schlüssel der **RfA**-CA wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
- Der Zertifikatsnehmer (die **RfA**-CA) ist nicht mehr berechtigt, das Zertifikat zu nutzen.
- Der Zertifikatsnehmer (die **RfA**-CA) hält die CP d. h. die Mindestanforderungen der Rundfunk-Root-CA nicht ein.

- Die **RfA**-CA hält die 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 Zertifikat 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 (1) angefertigt und in einem geschützten Laufwerksordner 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 (1) über den Sperrantrag, dessen Prüfung und den Entscheid an und legt sie in einem geschützten Laufwerksordner 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 (1) über den Vorgang an. Diese Protokollnotiz wird in einem geschützten Laufwerksordner der **RfA** PKI abgelegt und dort

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

(1) Eine schriftliche Protokollnotiz ist ein meist handgeschriebener Eintrag in einem Log-Protokoll, könnte aber auch elektronisch abgebildet werden, bspw. als Incident oder Change-Ticket im Ticketsystem.

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 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 auch 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 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 der Gültigkeit von **RfA** Sub-CA Zertifikaten an.

4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen

Zertifikatsprüfer müssen keine Online-Prüfungen von Sperrinformationen durchführen.

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 Bedingungen 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 Suspendierungen

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

4.10 Statusabfragedienst für Zertifikate

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

4.10.1 Funktionsweise des Statusabfragedienstes

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

4.10.2 Verfügbarkeit des Statusabfragedienstes

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

4.10.3 Optionale Leistungen

Die **RfA**-CA bietet keinen Statusabfragedienst an (siehe Kapitel 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 Bedingungen 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 HSMs und die Hosts für die Speicherung und den Betrieb der virtuellen Maschine der **RfA**-CA sind in Serverräumen - die durch geeignete physische Sicherheitsvorkehrungen einen ausreichenden Schutz vor äußeren Einflüssen gewährleisten - untergebracht.

Die Serverräume werden u. a. für den Betrieb von weiteren Systemen mit hohem Schutzbedarf der RfA genutzt. Die in den nachfolgenden Kapiteln aufgeführten baulichen Sicherheitsmaßnahmen (Zugang, Brandschutz etc.) sind daher – unabhängig von Ihrer Nutzung für die **RfA**-CA – bereits auf einen entsprechend hohen Schutzbedarf ausgerichtet.

5.1.2 Zugang

Die Räume in denen die redundanten HSMs sowie die redundanten Systeme, auf denen die virtuelle Maschine der **RfA**-CA gespeichert und bei Bedarf betrieben werden, befinden sich in Serverräumen, die wie folgt geschützt sind:

- Der Zutritt ist nur für berechtigte **RfA**-Mitarbeiter möglich.
- Die Räume sind verschlossen.
- Die HSM-Systeme selbst sind abgeschlossen mit einem eigenen physikalischen Sperrelement und zwei Sicherheitsschlössern.
- Es haben nur Mitarbeitender von Dienstleistern Zutritt, die durch die Abteilungsleitung einzeln autorisiert wurden und der entsprechenden Erklärung zum Datenschutz, zur Vertraulichkeit und zur Datenverarbeitung unterliegen.
- Grundsätzlich erfolgt ein ansonsten ggf. betrieblich ad hoc erforderlicher Zutritt von Personal eines Dienstleisters nur in Begleitung eines berechtigten RfA-Mitarbeiters.

5.1.3 Strom, Heizung und Klimaanlage

Die Stromversorgung und Klimatisierung ist für die Serverräume, in denen die Offline **RfA**-CA gespeichert und bei Bedarf betrieben wird, durch eine redundante Auslegung der Stromversorgung und Klimatisierung sichergestellt.

5.1.4 Wassergefährdung

Gefährdungen durch Wasser ist in den Serverräumen, in denen die **RfA**-CA gespeichert und bei Bedarf betrieben wird, hinreichend ausgeschlossen. Notfallmaßnahmen können ergriffen werden. Leckagesensoren überwachen die Serverräume. Sollte es zu einer Leckage kommen, erfolgt eine Alarmierung und es werden automatisch Absperrventile zugefahren.

5.1.5 Brandschutz

In den Serverräumen, in denen die **RfA**-CA gespeichert und bei Bedarf betrieben wird, ist ein geeigneter Brandschutz vorhanden.

Die beiden von der **RfA**-CA genutzten Serverräume befinden sich in unterschiedlichen Brandschutzabschnitten. Die Räume sind mit einem RAS-System (Rauchansaugsystem) ausgestattet, im Doppelboden werden zusätzlich punktförmige Rauchmelder eingesetzt. Bei einer Detektion des Systems wird automatisch die Feuerwehr alarmiert.

Der Disaster-Recovery-Tresor (vgl. Abschnitt 5.1.8) befindet sich in einem anderen Brandschutzabschnitt als die beiden Serverräume. Zudem ist der Tresor feuersicher.

5.1.6 Lager und Archiv

Datenträger mit sicherheitsrelevanten, vertraulichen oder personenbezogenen Daten werden vor unberechtigten Zugriffen geschützt im Tresor der Abteilung Infrastruktur aufbewahrt. Dieser Tresor befindet sich in einem Büro dar Abteilung Infrastruktur in einem anderen Brandschutzabschnitt als die Serverräume. Zudem ist der Tresor feuersicher.

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 wird täglich eine Sicherungskopie der virtuellen Maschine der RfA-CA erstellt und 3 Monate aufbewahrt. Für das Backupsystem gibt es ein Sicherheitskonzept. Es besteht u.a. eine geografische Trennung sowie eingeschränkter Netzwerkzugriff.Die Wiederherstellung der HSM Partitionen kann über ein sicher aufbewahrtes, zugangs- und passwortgeschütztes Backup HSM vorgenommen werden. Weiterhin kann eine wiederherzustellende Partition über ein intaktes, bereits in Betrieb genommenes HSM wiederhergestellt werden.

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:

Rolle	Typ der Rolle	Mindest-Anzahl Personen	Aufgabe der Rolle	Zuständig-keit	Kürzel
Lokaler Administrator der **RfA** Root-CA VM	Betriebssystem	2	Installation, Konfiguration, Administration und Wartung des Betriebssystems der RfA-CA Abbildung durch lokale Gruppen möglich Installation der AD Certificate Services lokale Administrationsrechte, Kenntnis der Boot- und Administrator-Passwörter der Systeme Erneuerung des lokalen Root-CA Zertifikats (erfordert Zugriff auf den Local Machine Certificate Store)	Mitarbeiter der **RfA** Abteilung Infra-struktur	LA
Zertifizierungsstellen-administrator	PKI	4	Konfiguriert und wartet die **RfA**-CA. konfiguriert Veröffentlichungspunkte der CA konfiguriert die Richtlinien- und Veröffentlichungsmodule	Mitarbeiter der **RfA** Abteilung Infra-struktur	CCA

			definiert für jeden Zertifikatsmanager die globalen Gruppen für die er zuständig ist definiert Zertifikatsmanager definiert Key Recovery Agents definiert weitere CA Administratoren löschen einzelner CA-Datenbank-Records aktivieren, veröffentlichen und konfigurieren der CRLs CA Konfiguration, lesen und für aktivierte Bereiche ändern starten und stoppen des Zertifikats-Dienstes zusätzlich möglich ist die Aktivierung der Konfiguration der Audit-Parameter Anlegen und Modifizieren von Zertifikatsvorlagen: z. B. Anpassungen in Bezug auf Namen, Laufzeit, Verwendungszweck und		

			Ausstellungsverhalten der Zertifikate Ist auch verantwortlich für die Zertifikats-ausstellung und ggf. -sperrung von Issuing-CAs. Übernimmt die Veröffentlichung der RfA-CA Sperrliste.		
Zertifikats-Manager	PKI	4	Entgegennahme von Zertifikat- und Sperranträgen. Beratung der Zertifikatnehmer Prüfung von Zertifikat- und Sperranträgen hinsichtlich Vollständigkeit und Korrektheit Ausstellen oder Verbieten wartender Zertifikatsanträge Sperren von Zertifikaten Zuweisung der KeyRecoveryAgent Zertifikate Recovery von Zertifikaten Extrahierung der private Key BLOB, welche im PKCS#7-	Mitarbeiter der **RfA** Abteilung Infra-struktur	CM

			Format verschlüsselt gespeichert sind Archivierung von Dokumenten		
Backup Operator	Betriebssystem	2	Zuständig für Backup und Wiederherstellung des Systems	Mitarbeiter der **RfA** Abteilung Infra-struktur	BO
Informationssicherheits-beauftragter (interne / externe Auditorrolle)	PKI	1	Durchführung der betriebsinternen Audits und 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	wird für Audits dem jeweiligen Auditor zugewiesen Mitarbeiter der **RfA** oder einer Fremdfirma	ISO

Tresorverwalter für Tresor IT	Schließregelung	4	Zugriff auf Tresor IT im 4-Augen-Prinzip. Dort werden verwahrt: Sicherungskopie von Schlüssel und Zertifikat der **RfA**-CA (HSM-Backup-System) Sicherungskopien der **RfA**-CA Datenbank und Log-Dateien Versiegelte Umschläge mit den Passworthälften für den Zugriff auf die privaten Schlüssel im HSM.	Mitarbeiter der **RfA** Abteilung Infra-struktur	TV1
Tresorverwalter für den lokalen persönlichen Password Safe der **RfA** Root-CA Administratoren	Schließregelung	je 1	Zugriff auf den persönlichen Password Safe. Dort werden verwahrt: Passworthälfte für den Zugriff auf die privaten Schlüssel im HSM Passwort des lokalen Administrators der **RfA** Root-CA VM Passwort des **RfA** Root-CA Administrator	Mitarbeiter der **RfA** Abteilung Infra-struktur	TV2

5.2.2 Mehraugenprinzip

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

Ein Vieraugenprinzip ist ebenfalls umgesetzt für den Zugriff auf den Tresor der Abteilung Infrastruktur mit allen Backup-Daten für ein Desaster-Recovery.

5.2.3 Identifizierung und Authentifizierung jeder Rolle

Die Authentifizierung der Rolle CAA1&2 (Zertifikatsstellenadministratoren) erfordert die Anmeldung mit einem zweigeteilten Passwort. Für alle weiteren Rollen erfolgt die Identifikation und Authentifizierung mit Benutzername und Passwort gemäß der RfA Passwortpolicy. Die Rolle der Tresorverwalter "TV1", "TV2" und "TV3" erfordert keine Authentifizierung an einem IT-System.

5.2.4 Rollentrennung

Für keine der Rollen der **RfA**-CA ist eine Aufgabentrennung umgesetzt.

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.

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 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 7 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

Das Log-Protokoll der **RfA**-CA wird im Rahmen des Backup regelmäßig gesichert.

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 in unregelmäßigen Abständen gepatcht.

Der Hypervisor-Cluster, auf dem die **RfA**-CA betrieben wird, dient auch als Plattform für weitere sicherheitskritische Serversysteme wie bspw. Datenbankserver. Daher wird dessen Betrieb unabhängig von der Nutzung durch die **RfA**-CA laufend überwacht.

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen

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

- Passwort des lokalen Systemadministrators der **RfA**-CA VM in einem versiegelten Umschlag
- Passwort der Sicherungskopie von Schlüssel und Zertifikat der **RfA**-CA in einem versiegelten Umschlag
- Sicherungskopie der virtuellen Maschine der **RfA**-CA
- Sicherungskopie von Schlüssel und Zertifikat der **RfA**-CA in einem Backup-HSM
- Zertifikats- und Sperranträge von **RfA** Sub-CAs an die **RfA**-CA

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

Folgende Sicherungskopien werden durch Verschlüsselung geschützt:

- Sicherungskopie von Schlüssel und Zertifikat der **RfA**-CA im Backup-HSM

Auf die Tresore haben nur benannte Tresorverwalter Zugriff.

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 ausgestellten 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.

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 des **RfA**s 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 Sicherungskopien der virtuellen Maschine, der private Schlüssel, die HSM Konfiguration und die zugehörige HSM-Partition 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

Das Schlüsselpaar der **RfA**-CA wurde unter Zeugen über den CSP auf der HSM erzeugt. Die **RfA**-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 Cryptoproviders 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 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

Das Prüfverfahren und die Anforderungen zur Prüfung des RSA Algorithmus inklusive der Schlüsselgenerierung sind vom NIST spezifiziert.

Die Qualität der erzeugten Public Key Parameter entspricht den Anforderungen aus FIPS 140-2. Die “Cryptographic Modules” (Cryptographic API Next Generation (CNG)) wurden von NIST – u.a. in Windows Server 2016 – erfolgreich nach FIPS 140-2 überprüft [3].

Die HSM (Safenet Luna SA7) erfüllen FIPS 140-2 Level 2 and Level 3 und NIST SP 800-131A.

[3] Siehe https://blogs.technet.microsoft.com/tip_of_the_day/2017/03/17/tip-of-the-day-fips-140-2-validation-of-windows-10-1607-and-windows-server-2016/

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

Es werden HSMs (Hardware Security Module) eingesetzt. Die HSM (Safenet Luna SA7) erfüllen FIPS 140-2 Level 2, Level 3 und NIST SP 800-131A.

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

Der private Schlüssel der **RfA**-CA wird niemals außerhalb der sicheren Grenzen des HSM im Klartext abgespeichert oder in anderer Weise zugänglich gemacht.

Der Zugriff auf die im HSM gespeicherten privaten Schlüssel ist ausschließlich mit Hilfe des aufgeteilten Passwortes möglich (4-Augen-Prinzip).

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

Der private Schlüssel wird durch den **Security-World** benannten Mechanismus der Safenet-Luna-SA7-HSM auf einer durch die Safenet-Luna-SA7-HSM gesicherten Partition auf einem System des **RfA**-CA-Verbundes gespeichert. Der private Schlüssel der **RfA**-CA wird niemals außerhalb der sicheren Grenzen des HSM im Klartext abgespeichert oder in anderer Weise zugänglich gemacht. Das Backup des privaten Schlüssels erfolgt mit der Sicherung auf einem Backup-HSM-System.

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

Die Übertragung des Schlüsselmaterials der **RfA**-CA zwischen den HSM erfolgt immer in verschlüsselter Form und wird niemals außerhalb der sicheren Grenzen des HSM im Klartext abgespeichert oder in anderer Weise zugänglich gemacht.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Der private Schlüssel wird durch den **Security-World** benannten Mechanismus der Safenet-Luna-SA7-HSM auf einer durch die Safenet-Luna-SA7-HSM gesicherten Partition auf einem System des **RfA**-CA-Verbundes gespeichert. Der private Schlüssel der **RfA**-CA wird niemals außerhalb der sicheren Grenzen des HSM im Klartext abgespeichert oder in anderer Weise zugänglich gemacht.

6.2.8 Aktivierung privater Schlüssel

Für den Start der PKI-Dienste der RfA-CA werden zwei RfA-CA-Administratoren benötigt, um die Partitionen des Safenet-Luna-SA7-HSM mittels zweigeteiltem Passwort mit der RfA-CA zu verbinden.

6.2.9 Deaktivierung privater Schlüssel

Der private Schlüssel der **RfA**-CA kann durch Beendigung des Zertifikatsdienstes oder Herunterfahren des Systems deaktiviert werden.

6.2.10 Zerstörung privater Schlüssel

Der private Schlüssel der **RfA**-CA kann durch die Software LunaCM des HSM-Herstellers sicher gelöscht werden.

6.2.11 Beurteilung kryptographischer Module

Es werden HSMs (Hardware Security Module) eingesetzt. Die HSM (Safenet-Luna-SA7-HSM) erfüllen FIPS 140-2 Level 2, Level 3 und NIST SP 800-131A.

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

Der Zugang zur **RfA**-CA erfolgt mit Username und Passwort gemäß den **RfA** Sicherheitsvorgaben (komplexes Kennwort mit mindestens 12 Zeichen). Für den Start der PKI-Dienste der **RfA**-CA werden zwei RfA-CA Administratoren benötigt mit ihren jeweiligen Passworthälften. Es sind 10 Fehlversuche erlaubt bis zur Sperrung der HSM-Partition.

6.4.2 Schutz von Aktivierungsdaten

Das Passwort der **RfA**-CA ist nur den CA-Administratoren bekannt. Für den Start der PKI-Dienste der RfA-CA siehe Kapitel 6.4.1

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) mit dem Betriebssystem Windows Server 2019, die als Offline-CA auf der redundanten VMware Infrastruktur der **RfA** betrieben wird. Die kryptografischen Prozesse erfolgen auf redundanten HSMs. Das in der VM eingesetzte Windows Server 2019 Betriebssystem wird entsprechend den hierfür gültigen Vorgaben der **RfA** (auf Basis BSI) installiert und gehärtet. Nicht benötigte Netzdienste wurden deaktiviert. Das Gastbetriebssystem verfügt ausschließlich über eine Netzwerkverbindung zu den redundanten HSMs und ist ein AD Mitglied. Das System ist ohne die Verbindung zu den HSMs, die nur über das Partitionspasswort aktiviert werden kann, nicht zur Ausstellung von Zertifikaten verwendbar. Ein Zugriff auf die Schlüssel wird durch die Verwendung der HSMs ausgeschlossen.

Die **RfA**-CA wird durch geeignete Benutzerauthentisierung und Zugriffskontrolle (Login mit Username und Kennwort gemäß den Sicherheitsregeln der **RfA**) vor unberechtigten Zugriffen geschützt. Sowohl der lokale Systemadministrator als auch die **RfA**-CA Administratoren haben ein Passwort bestehend aus mindestens zwölf 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 Safenet-Luna-SA7-HSM erfüllen FIPS 140-2 Level 2, Level 3 und NIST SP 800-131A.

6.6 Technische Maßnahmen während des Life Cycles

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

Es findet keine Software-Entwicklung statt.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Da die **RfA**-CA als Offline-CA meistens nicht in Betrieb ist, nur eingeschränkten Netzzugang für die HSMs hat, werden aktuelle Updates und Patches für die virtuelle Maschine der **RfA**-CA nur unregelmäßig eingespielt. Die VMware Infrastruktur der **RfA** ist in den regelmäßigen Patch- und Update- Managementprozess der **RfA** integriert.

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. Für die virtuelle Infrastruktur der **RfA und die HSMs** gelten während des Lebenszyklus die gleichen Sicherheitsmaßnahmen wie für alle anderen Serversysteme bei der **RfA** auch.

6.7 Sicherheitsmaßnahmen für Netze

Die **RfA**-CA wird als offline-CA betrieben, und hat zu dem dedizierten HSM-Netzwerk eine Verbindung.

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 nicht-kritisch 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 Unterkapitel 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 3 Monate nach der Aufnahme durchgeführt werden. Bei Bestandmitgliedern wählt der Betreiber mit geeignetem zeitlichen Vorlauf vor Erstellung des Jahresberichts mindestens zwei (innerhalb von 3 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 Kapitel 8.1 bis 8.6 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

Die **RfA**-CA verwendet keinen OID zur Kennzeichnung ihres Policy-Dokuments.

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 Hamburg als Sitz des Betreibers der **RfA**-CA.

9.16.5 Höhere Gewalt

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

9.17 Andere Bestimmungen

Es gibt keine weiteren Bestimmungen.

10. Anhang

Eine Änderung dieses Kapitel bedarf keiner Anpassung der Versionsnummer, es wird allerdings das Datum (Stand) des Dokumentes angepasst.

10.1 Kontaktdaten

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: **http(s)://ca-info.ndr.de**