Westdeutscher Rundfunk

WDR RfA-CA

Zertifizierungsrichtlinie und Regelungen für den Zertifizierungsbetrieb (CP/CPS)

Version 1.8
Datum 06. Juli 2018

Westdeutscher Rundfunk
Appellhofplatz 1
D-50667 Köln

www.wdr.de

Inhaltsverzeichnis

1 Einführung

1.1 Überblick

Die WDR PKI ist Teil der übergreifenden Zertifikatsinfrastruktur des gesamten ARD-Daten-CN, um gemeinsame PKI-Anwendungen über die Grenzen einzelner Rundfunkanstalten hinweg zu ermöglichen. Hierzu zählen im Besonderen der RfA-übergreifende WLAN-Zugang, die RfA-übergreifende SSL/TLS-Webserverauthentifikation und perspektivisch ein Austausch signierter und verschlüsselter E-Mails.

Zu diesem Zweck ist die WDR RfA-CA von der Rundfunk-Root-CA zertifiziert.

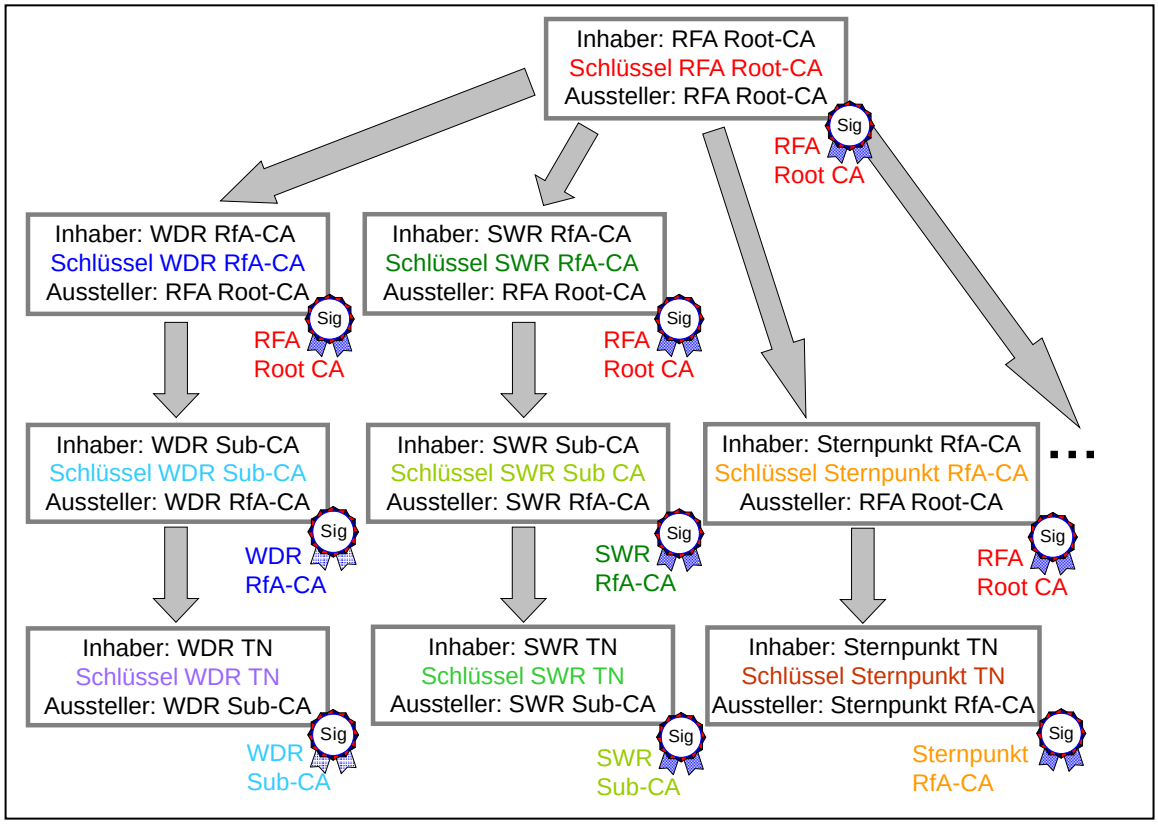

Abbildung 1: Zertifikatsinfrastruktur des ARD-Daten-CN

Dieses Dokument ist eine Kombination der Certificate Policy (CP) und der Certificate Practice Statement (CPS) der WDR RfA-CA. Es beschreibt den Zertifizierungsbetrieb der WDR RfA-CA sowie die Anforderungen an untergeordnete WDR Sub-CAs und stellt dar, wie die WDR RfA-CA die Mindestanforderungen der Rundfunk-Root-CA erfüllt.

Alle in diesem Dokument genannten Anforderungen sind für die WDR Sub-CAs verbindlich und können nicht abgeschwächt werden. Die Anforderungen betreffen die infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen und Abläufe innerhalb der WDR Sub-CAs und legen dabei insbesondere die Rahmenbedingungen für die Ausstellung von Zertifikaten entsprechend der internationalen Norm X.509 fest.

1.2 Name und Kennzeichnung des Dokuments

Name: Zertifizierungsrichtlinie und Regelungen für den Zertifizierungsbetrieb (CP/CPS) der WDR RfA-CA „WDR_RfA-CA_CP-CPS_Version _1_8.docx“

Bemerkung: Referenziert auf die Version Mindestanforderungen_RfA-CA_30

Version: 1.8

Datum: 06.07.2018

Überarbeitet: Hatice Tuncay, Andreas Hankel

1.3 Teilnehmer der Zertifizierungsinfrastruktur (PKI)

1.3.1 Zertifizierungsstellen

Beim WDR wird eine dreistufige Zertifikatsinfrastruktur-Hierarchie aufgebaut:

- Den Vertrauensanker der Zertifikatsinfrastruktur bildet die Rundfunk-Root-CA.
- Die Rundfunk-Root-CA zertifiziert die WDR RfA-CA. Aus WDR interner PKI-Sicht wird diese WDR RfA-CA auch als WDR Root-CA bezeichnet (siehe Abb. 2)
- Die WDR RfA-CA zertifiziert die WDR Sub-CA und ggf. zukünftig weitere untergeordnete Sub-CAs.
- Die WDR Sub-CA zertifiziert keine weiteren Sub-CAs.

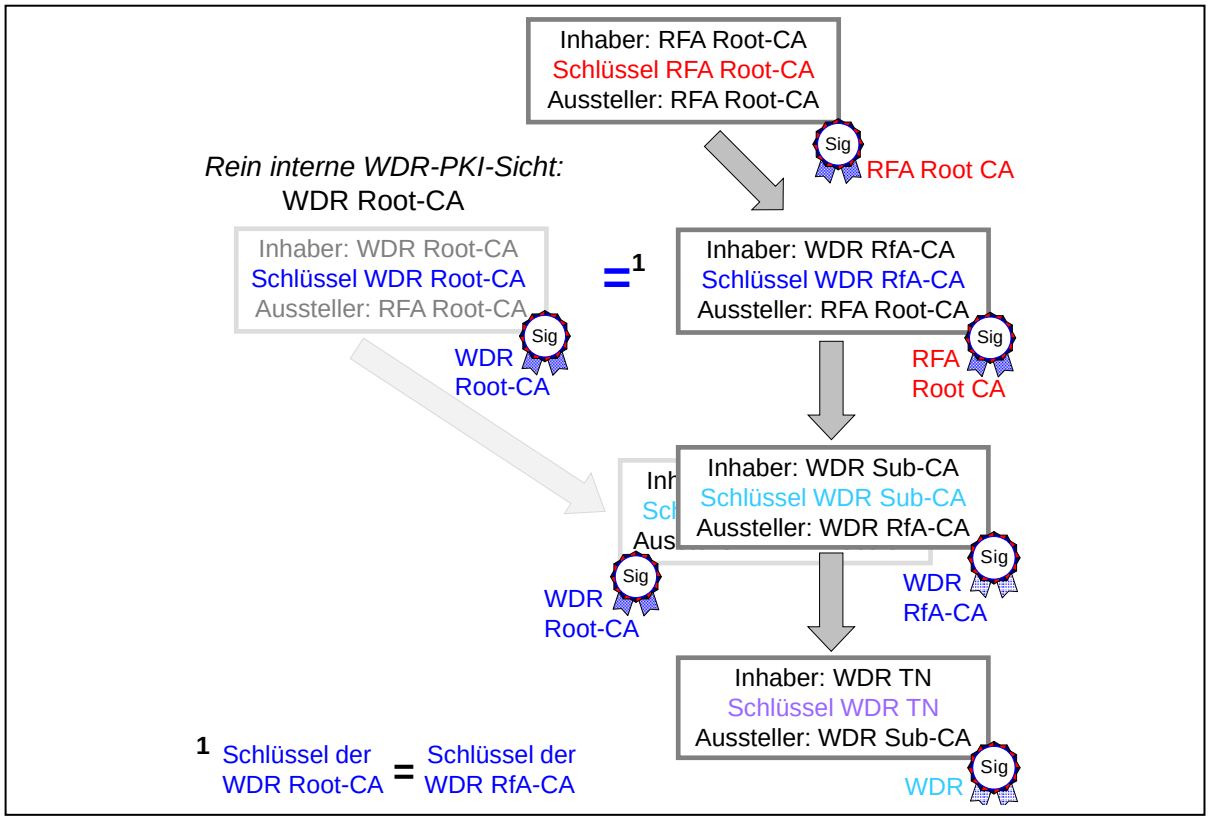

Abbildung 2: Überblick über die WDR-PKI

1.3.2 Registrierungsstellen

Die Registrierungsstelle heißt WDR RA und ist Bestandteil der WDR RfA-CA.

1.3.3 Zertifikatsinhaber (Subscribers)

Zertifikatsinhaber werden im Folgenden auch als Zertifikatsnehmer bezeichnet. Zertifikatsnehmer der WDR RfA-CA sind WDR Sub-CAs, die Zertifikate für natürliche Personen ausstellen. Diese Sub CAs dürfen keine weiteren untergeordneten Sub CAs ausstellen.

1.3.4 Zertifikatsprüfer (Relying Parties)

Zertifikatsprüfer sind alle Personen, Systeme und Organisationen, die Zertifikate von Zertifikatsnehmern nutzen.

1.3.5 Weitere Teilnehmer

CA-Steuerungsgruppe
Die WDR RfA-CA hat dem Betreiber der Rundfunk-Root-CA einen Vertreter benannt, der in der CA-Steuerungsgruppe der übergreifenden Zertifikatsinfrastruktur des gesamten ARD-Daten-CN teilnimmt. (aktueller Ansprechpartner: Rainer Birkendorf)

CA-Ansprechpartner
Die WDR RfA-CA hat dem Betreiber der Rundfunk-Root-CA einen CA-Ansprechpartner benannt und dessen Kontaktdaten der Rundfunk-Root-CA übermittelt. Dieser CA-Ansprechpartner steht dem Betreiber der Rundfunk-Root-CA als technischer Ansprechpartner zur Verfügung. (aktuelle Ansprechpartner: Peter Ladwig, Andreas Beer)

1.4 Anwendungsbereich

1.4.1 Geeignete Zertifikatsnutzung

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

Eine WDR Sub-CA darf nur Zertifikate für Personen, Maschinen oder Funktionsaccounts ausstellen. Sie muss die erlaubte Verwendung des ausgestellten Zertifikats mittels der Zertifikatserweiterung *KeyUsage* bzw. *ExtendedKeyUsage* kennzeichnen.

1.4.2 Untersagte Zertifikatsnutzung

Die WDR RfA-CA darf keine Endanwenderzertifikate ausstellen.

Eine WDR Sub-CA darf keine weiteren Sub-CA-Zertifikate ausstellen.

Sowohl die WDR RfA-CA als auch jede WDR Sub-CA dürfen ihre Schlüssel nicht zu Verschlüsselungs- oder Authentisierungszwecken oder für andere Signaturen als zur Zertifikats- oder Sperrlistenausstellung nutzen.

1.5 Verwaltung und Verantwortung der Zertifizierungsrichtlinie

1.5.1 Zuständigkeit für Zertifizierungsrichtlinie

Zuständig für dieses Dokument ist der Betreiber der WDR RfA-CA als Inhaber der Zertifizierungsrichtlinie.

1.5.2 Ansprechpartner/Kontaktperson

Die Kontaktperson ist der CA-Ansprechpartner, der beim Betreiber der Rundfunk-Root-CA benannt wurde.

1.5.3 Eignungsprüfer für Regelungen für den Zertifizierungsbetrieb (CPS) gemäß Zertifizierungsrichtlinie

Diese Zertifizierungsrichtlinie wird einmal im Jahr vom Betreiber der WDR RfA-CA auf Aktualität überprüft. Eine Auditierung der WDR RfA-CA findet jährlich gemäß der Vorgabe der Rundfunk-Root-CA durch den Sicherheitsbeauftragten des WDR statt (siehe Kapitel 8).

1.5.4 Annahmeverfahren für eine WDR Sub-CA

Eine WDR Sub-CA muss dem Betreiber der WDR RfA-CA bei Zertifikatsbeantragung ein CPS bzw. ein kombiniertes CP/CPS Dokument vorlegen, in dem der Zertifizierungsbetrieb und die Umsetzung der Anforderungen dieser Zertifizierungsrichtlinie beschrieben sind. Jede Sub-CA erfüllt die Mindestanforderungen der WDR-Root CA. Diese Mindestanforderungen werden nicht abgeschwächt.

Erfüllt eine WDR Sub-CA diese Anforderungen nicht, wird die Zertifizierung durch die WDR RfA-CA abgelehnt oder nachträglich widerrufen.

1.5.5 Zuständiger für die Anerkennung einer CP/CPS

Zuständig für die Anerkennung des CP/CPS einer WDR Sub-CA ist der IT-Sicherheits-beauftragte des WDR.

1.6 Begriffe und Abkürzungen

CA	**Certification Authority** Zertifizierungsstelle
CP	**Certificate Policy** Zertifizierungsrichtlinie
CPS	**Certification Practice Statement** Regelungen für den Zertifizierungsbetrieb
CSR	**Certificate Signing Request** Zertifikatsantrag
DN	**Distinguished Name** Vollqualifizierter Name
DNS	**Domain Name System** Namensauflösung im Internet
HTTPS	**Hypertext Transfer Protocol Secure** Sicheres Hypertext-Übertragungsprotokoll
IP	**Internet Protocol**
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

UPN	**User Principal Name** Eindeutiges Benennungsschema von Benutzer- und Computerobjekten im AD

2 Veröffentlichungen und Verzeichnisdienst

Die WDR RfA-CA stellt den Zertifikatsnutzern Sperrinformationen über Sperrlisten sowie das eigene von der Rundfunk-Root-CA ausgestellte WDR RfA-Zertifikat zur Verfügung. Dabei stellt der Betreiber der WDR RfA-CA sicher, dass die Veröffentlichung personenbezogener Daten nicht den geltenden Datenschutzrichtlinien widerspricht.

Werden die Zertifikate einer WDR Sub-CA für CN-weit angebotene Dienste verwendet, müssen diese nicht nur WDR-intern, sondern auch RfA-übergreifend geprüft werden können. Hierfür müssen das WDR Sub-CA-Zertifikat und die Sperrinformationen nicht nur im AD, sondern auch im Daten-CN verfügbar sein.

Ggf. kann eine WDR Sub-CA zukünftig auch für die Ausstellung von E-Mail-Zertifikaten für das beim WDR betriebene Secure E-Mail Gateway genutzt werden. Da E-Mail-Zertifikate nicht nur WDR-intern, sondern auch von Externen überprüfbar sein müssen, müssen in diesem Fall die CA-Zertifikate der Zertifikatskette und Sperrinformationen auch im Internet verfügbar gemacht werden.

WDR Sub-CAs müssen ihrerseits Sperrinformationen und ihr Sub-CA Zertifikat mindestens im AD des WDR veröffentlichen.

2.1 Verzeichnisdienste

Das Root-CA Zertifikat der Rundfunk-Root-CA, das WDR RfA-CA Zertifikat, sowie die Sperrliste der WDR RfA-CA werden im AD des WDR verteilt und können von dort aus dem internen Netz per LDAP abgerufen werden. Die WDR RfA-CA nutzt Verzeichnisdienste, deren ordnungsgemäßer Betrieb sichergestellt ist und die sich am aktuellen Stand der Technik orientieren. Diese Anforderung gilt ebenfalls für die Sub-CA.

Damit auch Systeme anderer Rundfunkanstalten die von der WDR RfA-CA erstellten WDR Sub-CA Zertifikate prüfen können, werden das WDR RfA-CA-Zertifikat und deren Sperrliste im Daten-CN veröffentlicht. Anwendungen, die nicht auf das AD zugreifen können, z. B. RADIUS Server, Firefox-Browser oder Browser auf Nicht-Windows-Computern, greifen ebenfalls auf das WDR RfA-CA-Zertifikat und deren Sperrliste auf einem Webserver im Daten-CN unter http://wdrmspki.wdr.cn.ard.de zu. Auf dieser Seite sind auch die Ansprechpartner für die WDR PKI genannt und dieses Policy-Dokument verfügbar.

Um auch externen Zertifikatsnutzern das WDR RfA-CA Zertifikat und seine Sperrliste zur Verfügung zu stellen, werden das Zertifikat der WDR RfA-CA und die Sperrliste im Internet zur Verfügung gestellt.

Die URLs für alle oben genannten Abrufmöglichkeiten des WDR RfA-CA Zertifikats und der Sperrliste werden von der WDR RfA-CA in die ausgestellten Zertifikate eingetragen. So stellt die WDR RfA-CA all ihren Zertifikatsnutzern in geeigneter Weise ihre Sperrinformationen und ihr CA-Zertifikate zur Verfügung. Diese Anforderungen gelten ebenfalls für die Sub-CA’s.

WDR Sub-CAs veröffentlichen die Sperrinformationen und ihr Sub-CA Zertifikat im AD des WDR und im Daten-CN.

2.2 Veröffentlichung von Zertifizierungsinformationen

Die Veröffentlichung des WDR RfA-CA Zertifikats im AD, im Daten-CN und im Internet wird einmalig nach der Installation der WDR RfA-CA ausgeführt.

Die Veröffentlichung der Sperrliste im Daten-CN und im Internet ist nach jeder Ausstellung einer neuen Sperrliste durch die WDR RfA-CA erforderlich.

Die Veröffentlichung des Fingerprints des WDR RfA-CA Zertifikats im AD, im Daten-CN und im Internet wird einmalig nach der Installation der WDR RfA-CA ausgeführt.

Diese Anforderungen gelten ebenfalls für die Sub-CAs.

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

Die Informationen werden rechtzeitig vor ihrem Ablauf aktualisiert. Die Sperrliste der WDR RfA-CA wird jährlich neu ausgestellt und ist 13 Monate lang gültig. Somit ergibt sich ein Monat Karenz für die manuelle Erstellung und Veröffentlichung der nächsten Sperrliste. Im Fall der Sperrung eines Zertifikats wird bereits früher eine neue Sperrliste ausgestellt und veröffentlicht, die auch wieder für 13 Monate gültig ist.

Die Veröffentlichung von Sperrinformationen erfolgt unverzüglich spätestens 24 Stunden nach durchgeführter Sperrung eines Zertifikates.

Die Anforderung nach einer unverzüglichen Veröffentlichung einer durchgeführten Sperrung (spätestens nach 24 Stunden) gilt auch für alle WDR Sub-CAs.

2.4 Zugangskontrolle zu Verzeichnisdiensten

Der lesende Zugriff auf die im Abschnitt 2.2 genannten Informationen ist ohne vorherige Anmeldung 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 des WDR RfA-CA Zertifikats und der WDR RfA-CA Sperrliste gewährleistet ist und ob sie von der Rundfunk-Root-CA bzw. der WDR RfA-CA als vertrauenswürdigem Herausgeber stammen. Diese Anforderungen gelten ebenfalls für die SUB-CAs.

3 Identifizierung und Authentifizierung

3.1 Namen

3.1.1 Namensformen

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

Der Name der WDR RfA-CA lautet: *CN=WDR-CA, O=Westdeutscher Rundfunk, C=DE*

Der Name der ersten WDR Sub-CA lautet: *CN=WDR Sub-CA 01, O=Westdeutscher Rundfunk, C=DE*

Weitere WDR Sub CAs werden fortlaufend nummeriert

3.1.2 Aussagekraft von Namen

Die von der WDR RfA-CA verwendeten Namen sind aussagekräftig und identifizieren den Zertifikatsinhaber eindeutig.

Auch die WDR Sub-CAs verwenden aussagekräftige Namen in den Endteilnehmerzertifikaten.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsinhaber

Es werden keine Pseudonyme verwendet.

Auch die WDR Sub-CAs dürfen keine Zertifikate auf Pseudonyme ausstellen, sondern jedes Endanwenderzertifikat muss den Namen des Zertifikatsinhabers (Person, Server oder

Maschine) enthalten und ist ihm so eindeutig zugeordnet. Zertifikate für Funktionsaccounts müssen den Namen der Funktion und ggf. die E-Mail Adresse des funktionsgebundenen E-Mail Accounts enthalten.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Die Distinguished Names im *subject* und *issuer* Feld des Zertifikats bezeichnen den Zertifikatsinhaber und -herausgeber. Die *SubjectAltName* Erweiterung kann weitere Namensformen für den Zertifikatsinhaber enthalten, wie bspw. E-Mail Adresse, UPN, DNS-Name oder IP-Adresse.

3.1.5 Eindeutigkeit von Namen

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

Bei der Ausstellung von Zertifikaten durch eine WDR Sub-CA muss bei der Vergabe von Namen sichergestellt sein, dass der gewählte DN innerhalb der ausstellenden Sub-CA eindeutig ist.

3.1.6 Anerkennung, Authentifizierung und Funktion von Warenzeichen

Innerhalb des WDR werden keine Namen in Zertifikaten verwendet, die Warenzeichen oder Markennamen verletzen.

3.2 Identitätsüberprüfung bei Neuantrag

3.2.1 Nachweis des Besitzes des privaten Schlüssels

Ein X.509 Zertifikat bindet einen öffentlichen Schlüssel an den Namen des Zertifikats-inhabers. Um sicherzustellen, dass der Antragsteller im Besitz des zugehörigen privaten Schlüssels ist, muss der Zertifikatsantrag (CSR) im Rahmen eines sicheren Zertifikats- und Schlüsselmanagement-Protokolls mit eben diesem privaten Schlüssel digital signiert werden.

Die WDR RfA-CA verwendet ihr selbstsigniertes Zertifikat bei der Zertifikatsbeantragung.

Der Zertifikatsantrag einer WDR Sub-CA bzw. eines WDR Endteilnehmers muss mit seinem privaten Schlüssel digital signiert sein.

3.2.2 Authentifizierung von Organisationszugehörigkeiten

Beim Zertifikatsantrag durch eine WDR Sub-CA oder einen Endteilnehmer muss keine Organisationszugehörigkeit überprüft werden.

3.2.3 Anforderungen zur Authentifizierung des Zertifikatsinhabers

Bei einer Zertifikatsbeantragung ist keine gesonderte Identitätsprüfung erforderlich, wenn die Authentifizierung des Antragstellers auf Basis bereits erfasster Daten erfolgt oder wenn der Antragsteller den PKI-Administratoren der WDR RfA-CA persönlich bekannt ist. Ansonsten ist beim Neuantrag auf Zertifizierung eine gesonderte Identitätsprüfung des Antragstellers durchzuführen (siehe Kapitel 4.2.1).

Die Authentifizierung der Antragsteller bei der Beantragung von Endteilnehmerzertifikaten soll auf bereits beim WDR erfassten Daten basieren. Somit sind keine gesonderte Identitäts-prüfung und Authentifizierung des Zertifikatsinhabers bei einem Neuantrag für ein Endteilnehmerzertifikat erforderlich.

3.2.4 Nicht überprüfte Teilnehmerangaben

Es gibt keine nicht geprüften Teilnehmerangaben.

3.2.5 Überprüfung der Berechtigung

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

Eine WDR Sub-CA stellt Zertifikate nur nach Prüfung der Berechtigung des Antragstellers aus. Hierbei kann die Berechtigungsprüfung eines Antragstellers automatisch und auch schon vorab erfolgen, so dass nur berechtigte Nutzer überhaupt einen Zertifikatsantrag stellen können. Eine Sonderform eines berechtigten Nutzers ist das beim WDR betriebene Secure Web Gateway (Blue Coat), das die SSL/TLS-Verbindung von einem WDR Nutzer zu einem SSL/TLS-Server im Internet aufbricht. Dieser Proxy ist berechtigt, stellvertretend für beliebige SSL/TLS Server im Internet temporär gültige Serverzertifikate bei der WDR Blue Coat Sub-CA zu beantragen.

Der Prozess für die Prüfung der Berechtigung zur Antragsstellung muss von der Sub-CA in einem CPS bzw. in einem kombinierten CP/CPS Dokument dokumentiert sein.

3.2.6 Kriterien für Zusammenarbeit

Für eine übergreifende Zusammenarbeit müssen fremde Zertifikatsinfrastrukturen die Mindestanforderungen der Rundfunk-Root-CA erfüllen.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Im Unterschied zu einem Neuantrag zur Zertifizierung mit gesonderter Identitätsprüfung, muss bei einer Zertifikatserneuerung keine gesonderte Identitätsprüfung erfolgen, wenn die Authentifizierung des Antragstellers auf Basis seines noch gültigen Zertifikats erfolgt. Ist das Zertifikat jedoch schon abgelaufen, gelten bei der Zertifikatserneuerung die gleichen Identifizierungs- und Authentifizierungsanforderungen wie beim Neuantrag.

Ist beim Neuantrag keine gesonderte Identitätsprüfung erforderlich, so gilt dies ebenso für Anträge zur Zertifizierung nach einer Schlüsselerneuerung.

Diese Anforderung gilt ebenfalls auch für die WDR Sub-CAs und ist in einem kombinierten CP/CPS Dokument zu dokumentieren.

3.3.2 Zertifikatserneuerung nach einer Sperrung

Wurde das Zertifikat gesperrt, gelten bei der Zertifikatserneuerung die gleichen Identifizierung- und Authentifizierungsanforderungen wie beim Neuantrag. Ist beim Neuantrag keine gesonderte Identitätsprüfung erforderlich, so gilt dies ebenso für Anträge zur Zertifizierung nach einer Sperrung.

Diese Anforderung gilt ebenfalls auch für die WDR Sub-CAs und ist in einem kombinierten CP/CPS Dokument zu dokumentieren.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Bei einem Sperrantrag für eine WDR Sub-CA oder ein WDR Endteilnehmerzertifikat ist keine gesonderte Identitätsprüfung durch die ausstellende CA erforderlich, wenn der Antragsteller

den PKI-Administratoren der WDR RfA-CA bzw. der WDR Sub-CA persönlich bekannt ist. Ansonsten ist eine geeignete Identitätsprüfung des Antragstellers durchzuführen.

4 Ablauforganisation

4.1 Zertifikatsantrag

4.1.1 Wer kann ein Zertifikat beantragen

Die WDR RfA-CA stellt nur Zertifikate für WDR Sub-CAs aus. Ein Sub-CA-Zertifikat darf nur vom PKI-Ansprechpartner einer WDR Organisationseinheit oder seinem Vertreter beantragt werden.

Eine WDR Sub-CA darf nur Zertifikate für Endteilnehmer ausstellen, d.h. für WDR-Mitarbeiter, für externe Mitarbeiter, die für den WDR arbeiten, für interne Server, Maschinen und Geräte des WDR sowie für SSL/TLS Server, die von dem WDR Blue Coat Proxy beantragt werden. Ein solches Zertifikat für Endteilnehmer wird grundsätzlich durch den Zertifikatsnehmer bzw. eine autorisierte Person[1] oder ein autorisiertes System beantragt.

4.1.2 Verfahren und Zuständigkeiten

Der Antragssteller einer WDR Sub-CA muss lokal ein Schlüsselpaar erzeugen und anschließend den öffentlichen Schlüssel gesichert in einem Zertifikatsantrag (CSR) bei der WDR RfA-CA einreichen.

Der Zertifikatsantrag einer WDR Sub-CA wird auf vertrauenswürdigem Wege an die PKI-Administratoren der WDR RfA-CA übermittelt. Zulässig ist die Beantragung via E-Mail mit Rückruf an die vorab angegebene Telefonnummer des PKI-Ansprechpartners oder seines Vertreters oder die persönliche Übergabe eines Transfer-Datenträgers. Im Fall der persönlichen Übergabe muss eine Ausweisprüfung erfolgen, sofern der Antragsteller nicht persönlich bekannt ist.

4.2 Bearbeitung von Zertifikatsanträgen

4.2.1 Durchführung von Identifikation und Authentifizierung

Bei einer Zertifikatsbeantragung durch eine WDR Sub-CA ist keine gesonderte Identitätsprüfung erforderlich, wenn die Authentifizierung des Antragstellers auf Basis bereits erfasster Daten erfolgt oder wenn der Antragsteller den PKI-Administratoren der WDR RfA-CA persönlich bekannt ist. Ansonsten ist bei einem Neuantrag auf Zertifizierung eine Ausweisprüfung des Antragstellers durchzuführen. Die erfolgte Identitätsprüfung wird im vorhandenen Ticketsystem dokumentiert.

Die Authentifizierung der Antragsteller bei der Beantragung von Endteilnehmerzertifikaten soll auf bereits beim WDR erfassten Daten basieren. Somit ist keine gesonderte Identitätsprüfung erforderlich.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Die PKI Administratoren der WDR RfA-CA entscheiden nach Vorlage eines Zertifikatsantrags einer WDR Sub-CA über die Annahme oder Ablehnung des Antrags. Hierfür prüfen sie das CPS oder das kombinierte CP/CPS-Dokument der WDR Sub-CA, ob die Anforderungen aus diesem kombinierten CP/CPS-Dokument von der WDR Sub-CA erfüllt werden.

[1] Bspw. für SSL/TLS-Server

Zertifikatsanträge für Endteilnehmerzertifikate sollen möglichst aus bereits erfassten Daten generiert werden, so dass die Zertifikate automatisch ausgestellt werden können. Somit müssen die Zertifikatsanträge von den PKI Administratoren einer WDR Sub-CA nicht geprüft, angenommen oder abgelehnt werden. Nur Zertifikatsanträge mit selbst erfassten Daten im Antrag – wie typischerweise bei SSL/TLS-Serverzertifikaten – müssen von den PKI Administratoren einer WDR Sub-CA geprüft und angenommen oder bei Inkonsistenzen wie bspw. einem falschen Servernamen oder einer falschen IP-Adresse ablehnt werden. Die WDR Sub-CA muss in ihrem CPS oder kombinierten CP/CPS-Dokument darlegen, welche Prüfungen sie bei Zertifikatsanträgen mit selbst erfassten Daten im Zertifikatsantrag durchführt und wann sie Zertifikatsanträge ablehnt.

4.2.3 Bearbeitungsdauer bei Zertifikatsanträgen

Die Bearbeitungsdauer für Sub-CA Zertifikatsanträge ist nicht festgelegt.

Es bestehen von Seiten der WDR RfA-CA auch keine Anforderungen an WDR Sub-CAs für die Bearbeitungsdauer von Anträgen für Endteilnehmerzertifikate.

4.3 Zertifikatserstellung

4.3.1 Aufgaben der Zertifizierungsstelle

Die Ausstellung eines WDR Sub-CA Zertifikats durch die WDR RfA-CA ist nur im Vier-Augen-Prinzip zulässig. Eine Ausgabe von Zertifikaten durch die WDR Rfa-CA und der WDR Sub-CA gilt nur für gültige Zertifikatsanträge, die syntaktisch korrekt sind und alle erforderlichen Informationen im Antrag enthalten.

Nach Ausstellung des WDR Sub-CA Zertifikats fertigen die beiden beteiligten PKI-Administratoren der WDR RfA-CA eine schriftliche Protokollnotiz über den Vorgang an und archivieren diese in geeigneter Form.

Nach Ausstellung eines WDR Sub-CA-Zertifikats wird ein manuelles Backup der WDR RfA-CA Datenbank und der Log-Dateien erstellt. Die beiden beteiligten PKI-Administratoren der WDR RfA-CA brennen bzw. überwachen das Brennen der Backup-Daten auf ein optisches Speichermedium und übergeben diesen Datenträger anschließend gemeinsam dem zuständigen Tresorverwalter, der ihn im Tresor 3 beim WDR verwahrt.

Bei der Ausstellung von Endteilnehmerzertifikaten durch eine WDR Sub-CA ist kein Vier-Augen-Prinzip erforderlich. Eine WDR Sub-CA darf Endteilnehmerzertifikate automatisch ausstellen, wenn sie im Verzeichnisdienst als authorisierte Endteilnehmer authentifiziert sind. Eine Ausgabe von Endanwenderzertifikaten gilt nur für gültige Zertifikatsanträge in der WDR Sub-CA, die syntaktisch korrekt sind und alle erforderlichen Informationen im Antrag enthalten.

Die Authentifizierung der Antragsteller bei der Beantragung von Endteilnehmerzertifikaten soll auf bereits beim WDR erfassten Daten basieren. Somit ist keine gesonderte Identitäts-prüfung erforderlich.

Die eindeutige Verbindung zwischen dem Schlüsselpaar und dem Zertifikatsnehmer wird durch die Signatur geprüft. Die gleichen Bedingungen gelten auch für die WDR Sub-CAs und sollen im CP/CPS Dokument beschrieben sein.

4.3.2 Benachrichtigung des Antragstellers

Keine weiteren Festlegungen. Es findet keine zusätzliche Benachrichtigung statt.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme des Zertifikats

Es gibt keinen dedizierten Prozess zur Zertifikatsannahme durch die PKI-Administratoren der WDR Sub-CA.

Auch für die Endteilnehmer ist kein dedizierter Prozess zur Zertifikatsannahme erforderlich.

4.4.2 Veröffentlichung des Zertifikats durch die Zertifizierungsstelle

Die WDR RfA-CA veröffentlicht ihr Zertifikat im AD, im Daten-CN und im Internet.

Die WDR Sub-CAs müssen ihrerseits ihr CA-Zertifikat und ggf. die Verschlüsselungszertifikate für Benutzer so veröffentlichen, dass diese Daten-CN-weit abgerufen werden können.

4.4.3 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Es findet keine Benachrichtigung weiterer Instanzen statt.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Nutzung durch den Zertifikatsinhaber

Die WDR RfA-CA nutzt ihren Schlüssel und ihr Zertifikat nur für die im Zertifikat genannten Verwendungszwecke, d.h. zur Ausstellung von WDR Sub-CA Zertifikaten und Sperrlisten. Der private Schlüssel der WDR RfA-CA liegt geschützt auf einer produktiven Smartcard und drei Ersatzkarten, die bei Nichtgebrauch in einem Tresor beim WDR verwahrt werden.

Auch eine WDR Sub-CA oder ein Endteilnehmer darf seinen Schlüssel und Zertifikat nur für die im Zertifikat genannten Verwendungszwecke einsetzen. Er muss Sorge tragen, dass sein privater Schlüssel angemessen geschützt ist und das Zertifikat in Übereinstimmung mit dem CP/CPS der ausstellenden CA eingesetzt wird.

Das Zertifikat einer WDR Sub-CA wird von der WDR RfA-CA unverzüglich gesperrt, wenn die Angaben des Zertifikats nicht mehr korrekt sind oder wenn der private Schlüssel der WDR Sub-CA für unerlaubte Zwecke eingesetzt, abhandengekommen, gestohlen oder möglicherweise kompromittiert wurde.

Auch das Zertifikat eines Endteilnehmers ist unverzüglich von einer WDR Sub-CA zu sperren, wenn die Angaben des Zertifikats nicht mehr korrekt sind oder wenn der private Schlüssel des Endteilnehmers für unerlaubte Zwecke eingesetzt, abhandengekommen, gestohlen oder möglicherweise kompromittiert wurde.

Bietet eine WDR Sub-CA keine Möglichkeit der Schlüsselhinterlegung für Verschlüsselungsschlüssel des Zertifikatsnehmers an oder wird eine optionale Schlüsselhinterlegungsmöglichkeit bei der WDR Sub-CA vom Zertifikatsnehmer nicht in Anspruch genommen, so ist der Zertifikatsnehmer selbst dafür zuständig, seinen privaten Verschlüsselungsschlüssel so zu sichern, dass er ggf. verschlüsselte Daten wieder entschlüsseln kann.

4.5.2 Nutzung des Zertifikats durch die Relying Party

Ein Zertifikatsprüfer (engl.: Relying Party) darf ein Zertifikat nur für die im Zertifikat genannten Verwendungszwecke akzeptieren.

4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (Re-Zertifizierung)

4.6.1 Bedingungen für eine Zertifikatserneuerung

Eine Zertifikatserneuerung unter Beibehaltung des alten WDR RfA-CA Schlüssels findet nicht statt. Mit der Erneuerung des WDR RfA-CA Zertifikats werden auch neue Schlüssel erzeugt (siehe Abschnitt 4.7). Im Fall einer Zertifikatserneuerung für eine WDR Sub-CA oder einen Endteilnehmer muss in jedem Fall auch zwingend eine Schlüsselerneuerung stattfinden (siehe Abschnitt 4.7).

4.6.2 Wer darf eine Zertifikatserneuerung beantragen

Eine Zertifikatserneuerung unter Beibehaltung des alten WDR RfA-CA Schlüssels findet nicht statt. Es gelten die gleichen Regelungen wie bei einer Neubeantragung und sind im Kapitel 4.3 dokumentiert.

4.6.3 Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung

Eine Zertifikatserneuerung unter Beibehaltung des alten WDR RfA-CA Schlüssels findet nicht statt. Es gelten die gleichen Regelungen wie bei einer Neubeantragung und sind im Kapitel 4.3 dokumentiert.

4.7 Schlüssel- und Zertifikatserneuerung

Bei einer Zertifikatserneuerung mit Schlüsselwechsel wird einem Zertifikatsnehmer, der bereits ein Zertifikat besitzt, durch die zuständige CA ein neues Zertifikat für ein neues Schlüsselpaar ausgestellt, sofern die im Zertifikat enthaltenen Informationen unverändert bleiben. Dies betrifft die WDR RfA-CA, WDR Sub-CAs und Endteilnehmer beim WDR gleichermaßen.

4.7.1 Gründe für eine Schlüssel- und Zertifikatserneuerung

Grund für eine Schlüssel- und Zertifikatserneuerung ist der bevorstehende Ablauf eines Zertifikats.

Eine Schlüssel- und Zertifikatserneuerung muss auch stattfinden, wenn ein Zertifikat widerrufen wurde, aber ein entsprechendes Zertifikat weiterhin benötigt wird.

Eine Schlüssel- und Zertifikatserneuerung muss auch stattfinden, wenn ein Zertifikat aufgrund von Schlüsselkompromittierung gesperrt wurde.

Dies gilt ebenso für die WDR Sub-CAs und ist im kombiniertem CP/CPS Dokument dokumentiert.

4.7.2 Wer kann eine Schlüssel- und Zertifikatserneuerung beantragen

Es gelten die gleichen Regelungen wie bei einer Neubeantragung und sind im kombiniertem CP/CPS Dokument dokumentiert

4.7.3 Ablauf der Schlüssel- und Zertifikatserneuerung

Es gelten die gleichen Regelungen wie bei einer Neubeantragung und sind im Kapitel 4.3 dokumentiert.

4.7.4 Benachrichtigung des Zertifikatsinhabers

Die PKI-Administratoren einer WDR Sub-CA werden nicht von den PKI-Administratoren der WDR RfA-CA über den Ablauf ihres CA-Zertifikats und eine notwendige Zertifikats-erneuerung benachrichtigt.

Ob die Endteilnehmer von den PKI-Administratoren einer WDR Sub-CA über den bevorstehenden Ablauf ihres Zertifikats informiert werden, muss die WDR Sub-CA in ihrem CPS oder kombinierten CP/CPS-Dokument regeln. Es besteht keine Anforderung von Seiten der WDR RfA-CA an WDR Sub-CAs für eine solche Benachrichtigung.

4.7.5 Annahme der Schlüssel- und Zertifikatserneuerung

Es gibt keinen dedizierten Prozess zur Annahme der Schlüssel- und Zertifikatserneuerung durch die PKI-Administratoren der WDR Sub-CA.

Auch für die Endteilnehmer ist kein dedizierter Prozess zur Zertifikatsannahme erforderlich.

4.7.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle

Es gelten die gleichen Regelungen wie bei einer Neubeantragung.

4.7.7 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Es findet keine Benachrichtigung weiterer Instanzen statt.

4.8 Zertifikatsänderung

4.8.1 Gründe für eine Zertifikatsänderung

Haben sich Angaben in einem Zertifikat geändert, so muss eine Zertifikatsänderung beantragt und durchgeführt werden. Dies betrifft die WDR RfA-CA, WDR Sub-CAs und Endteilnehmer beim WDR gleichermaßen. Gründe für eine Zertifikatsänderung sind zum Beispiel:

- der Name des Zertifikatsnehmers hat sich nach Heirat/Scheidung geändert,
- die Zuordnung der im Zertifikat enthaltenen E-Mail-Adresse zum Zertifikatsnehmer ist nicht mehr gegeben.

4.8.2 Wer kann eine Zertifikatsänderung beantragen

Es gelten die gleichen Regelungen wie bei einer Neubeantragung.

4.8.3 Ablauf der Zertifikatsänderung

Eine Zertifikatsänderung bedeutet technisch die Sperrung des alten Zertifikats und die Ausstellung eines neuen Zertifikats. Für den Ablauf gelten die gleichen Regelungen wie in Abschnitt 4.9 und 4.7 beschrieben.

Es gelten die gleichen Regelungen in den WDR Sub-CAs und sind im kombiniertem CP/CPS Dokument dokumentiert.

4.8.4 Benachrichtigung des Zertifikatsinhabers

Die PKI-Administratoren einer WDR Sub-CA werden nicht von den PKI-Administratoren der WDR RfA-CA über eine Zertifikatsänderung benachrichtigt.

Auch für die Endteilnehmer ist keine Benachrichtigung von der WDR Sub-CA über eine Zertifikatsänderung erforderlich.

4.8.5 Annahme der Zertifikatsänderung

Es gibt keinen dedizierten Prozess zur Annahme der Zertifikatsänderung durch die PKI-Administratoren der WDR Sub-CA.

Auch für die Endteilnehmer ist kein dedizierter Prozess zur Annahme einer Zertifikatsänderung erforderlich.

4.8.6 Veröffentlichung einer Zertifikatsänderung durch die Zertifizierungsstelle

Es gelten die gleichen Regelungen wie bei einer Neubeantragung.

4.8.7 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Es findet keine Benachrichtigung weiterer Instanzen statt.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Gründe für eine Sperrung

Die WDR RfA-CA beantragt den Widerruf ihres eigenen RfA-CA Zertifikats bei der Rundfunk-Root-CA bzw. sperrt ein WDR-Sub-CA Zertifikat, wenn mindestens einer der folgenden Gründe vorliegt:

- Das Zertifikat enthält Angaben, die nicht mehr gültig sind.
- Der private Schlüssel des Zertifikatsnehmers wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
- Die WDR Sub-CA stellt den Zertifizierungsbetrieb ein.
- Die WDR Sub-CA hält Anforderungen aus diesem CP/CPS nicht ein.
- Die WDR RfA-CA hält die Regelungen dieser CP/CPS und damit die Mindest-anforderungen der Rundfunk-Root-CA nicht ein; somit sollten auch die WDR Sub-CA Zertifikate gesperrt werden.
- Der Zertifikatsnehmer ist nicht mehr berechtigt, das Zertifikat zu nutzen.
- Der Zertifikatsnehmer benötigt das Zertifikat nicht mehr.

Das Zertifikat eines WDR Endteilnehmers muss von der zuständigen WDR Sub-CA widerrufen werden, wenn mindestens einer der folgenden Fälle vorliegt:

- Das Zertifikat enthält Angaben, die nicht mehr gültig sind.
- Der private Schlüssel des Zertifikatsnehmers wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
- Die WDR Sub-CA stellt den Zertifizierungsbetrieb ein.
- Die Endteilnehmer hält Anforderungen aus diesem CP/CPS nicht ein
- Die WDR Sub-CA hält die Regelungen ihres CP/CPS nicht ein; somit sollten auch alle von ihr ausgestellten Endteilnehmerzertifikate gesperrt werden.
- Der Zertifikatsnehmer ist nicht mehr berechtigt, das Zertifikat zu nutzen.
- Der Zertifikatsnehmer benötigt das Zertifikat nicht mehr.

4.9.2 Wer kann eine Sperrung beantragen

Sperrberechtigt für ein WDR Sub-CA Zertifikat ist der zuständige PKI-Administrator der betroffenen WDR Sub-CA sowie sein Vertreter. Auch der PKI-Administrator der WDR RfA-CA kann mit Einverständnis des IT-Sicherheitsbeauftragten eine Sperrung beantragen, wenn bspw. die Mindestanforderungen aus dem CP/CPS der WDR PKI durch eine WDR Sub-CA nicht zuverlässig eingehalten werden.

Die Sperrberechtigung für Endteilnehmerzertifikate muss eine WDR Sub-CA in ihrem CPS oder kombinierten CP/CPS dokumentieren.

4.9.3 Ablauf einer Sperrung

Bei Verdacht auf Kompromittierung eines WDR Sub-CA Schlüssels oder bei Einstellung des Betriebs einer WDR Sub-CA stellt der PKI-Administrator der Sub-CA oder sein Vertreter einen Sperrantrag bei der WDR RfA-CA.

Eine Sperrung von WDR Sub-CA Zertifikaten durch die WDR RfA-CA darf nur im Vier-Augen-Prinzip erfolgen, d. h. durch zwei der PKI-Administratoren der WDR RfA-CA. Nach der Sperrung eines Sub-CA Zertifikats und der Ausstellung einer neuen Sperrliste fertigen die beiden beteiligten PKI-Administratoren der WDR RfA-CA eine schriftliche Protokollnotiz über den Vorgang an und archivieren diese in geeigneter Form.

Abschließend muss die neue Sperrliste exportiert und im Daten-CN und im Internet publiziert werden.

Nach Sperrung eines WDR Sub-CA-Zertifikats wird ein manuelles Backup der WDR RfA-CA Datenbank und der Log-Dateien erstellt. Die beiden beteiligten PKI-Administratoren der WDR RfA-CA brennen bzw. überwachen das Brennen der Backup-Daten auf ein optisches Speichermedium und übergeben diesen Datenträger anschließend gemeinsam dem zuständigen Tresorverwalter, der ihn im Tresor 3 beim WDR verwahrt.

Den Ablauf einer Sperrung von Endteilnehmerzertifikaten durch eine WDR Sub-CA muss von der WDR Sub-CA in ihrem CPS oder kombinierten CP/CPS dokumentiert werden.

4.9.4 Fristen für den Zertifikatsinhaber

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

Bei Bekanntwerden eines Sperrgrundes muss auch von einer WDR Sub-CA und einem Endteilnehmer unverzüglich die Sperrung bei der zuständigen Zertifizierungsstelle beantragt werden.

4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle

Die WDR RfA-CA führt die beantragte Sperrung des Zertifikats innerhalb von einem Arbeitstag durch.

Die Bearbeitungsfrist für die Sperrung von Endteilnehmerzertifikaten soll von der WDR Sub-CA in ihrem CPS oder kombinierten CP/CPS dokumentiert und wird innerhalb eines Arbeitstages durchgeführt werden.

4.9.6 Anforderung zu Sperrprüfungen durch eine Relying Party

Ein Zertifikatsprüfer prüft bei jedem Einsatz die Gültigkeit der Zertifikate. Hierzu prüft er die aktuelle Sperrliste oder bezieht eine OCSP-Auskunft und prüft diese auf das verwendete Zertifikat. Die gleichen Bedingungen gelten ebenfalls für die WDR Sub-CAs.

4.9.7 Häufigkeit der Sperrlistenveröffentlichung

Im Falle einer Sperrung eines Zertifikats wird zusätzlich eine neue Sperrliste ausgestellt und veröffentlicht.

Eine Sperrliste der WDR RfA-CA ist 13 Monate gültig und wird im Regelfall alle 12 Monate neu erstellt und veröffentlicht. Der 13. Monat dient als Karenzzeit für die Ausstellung und Veröffentlichung einer neuen Sperrliste.

Bei diesem jährlichen Zugriff auf die Tresore, in denen das Notebook mit der virtuellen Maschine der WDR RfA-CA und die produktive CA-Smartcard verwahrt werden, wird gleichzeitig auch die Unversehrtheit der versiegelten Umschläge mit den Smartcards, PINs, PUKs und Passwörtern geprüft und dokumentiert. Kontrolliert wird die Unversehrtheit durch den zuständigen Tresorverwalter gemeinsam mit den beiden WDR RfA-CA Administratoren.

Die Sperrliste einer WDR Sub-CA darf maximal 14 Tage gültig sein. Es ist mindestens wöchentlich (alle sieben Tage) eine neue Sperrliste zu erstellen.

Es gelten die gleichen Regelungen in den WDR Sub-CAs und sind im kombiniertem CP/CPS Dokument dokumentiert.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die maximale Latenzzeit für Sperrlisten (Zeitpuffer zwischen Erstellung und Veröffentlichung der Sperrlisten) beträgt ein Monat.

Die maximale Latenzzeit für Sperrlisten darf bei WDR Sub-CAs maximal 24 Stunden betragen, d. h. die Sperrliste darf maximal einen Tag länger gültig sein als der Ausstellungszyklus der Sperrliste.

4.9.9 Verfügbarkeit von Online-Statusabfragen (OCSP)

Die WDR RfA-CA bietet keinen Online-Dienst zur Auskunft der Gültigkeit von Zertifikaten an. Eine WDR Sub-CA kann einen solchen OCSP-Dienst zusätzlich oder alternativ zur Verwendung von Sperrlisten anbieten.

4.9.10 Anforderungen an Online-Statusabfragen (OCSP)

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

Bestehende Anforderungen an Online-Statusabfragen für Zertifikate einer WDR Sub-CA müssen von der WDR Sub-CA in ihrem CPS oder kombinierten CP/CPS dokumentiert werden.

4.9.11 Andere verfügbare Formen der Widerrufsbekanntmachung

Es gibt bei der WDR RfA-CA keine weiteren Formen der Widerrufsbekanntmachung.

Wenn eine WDR Sub-CA über andere Formen der Widerrufsbekanntmachung verfügt, müssen diese von der WDR Sub-CA in ihrem CPS oder kombinierten CP/CPS dokumentiert werden.

4.9.12 Anforderungen bei Kompromittierung von privaten Schlüsseln

Bei Kompromittierung eines privaten Schlüssels wird das zugehörige Zertifikat unverzüglich von der WDR RfA-CA widerrufen und umgehend – auch außerhalb des regulären Rhythmus – eine neue Sperrliste veröffentlicht.

Diese Anforderung gilt ebenso für WDR Sub-CAs.

4.9.13 Gründe für eine Suspendierung

Eine temporäre Sperrung bzw. eine Suspendierung von Zertifikaten durch die WDR RfA-CA ist verboten.

Es gelten die gleichen Regelungen in den WDR Sub-CAs und sind im kombiniertem CP/CPS Dokument dokumentiert

4.9.14 Wer kann Suspendierung beantragen

Eine Suspendierung von Zertifikaten findet bei der WDR RfA-CA nicht statt.

Wenn eine WDR Sub-CA Endteilnehmerzertifikate suspendiert, muss sie in ihrem CPS oder kombinierten CP/CPS dokumentieren, wer eine Suspendierung beantragen kann.

4.9.15 Ablauf einer Suspendierung

Eine Suspendierung von Zertifikaten findet bei der WDR RfA-CA nicht statt.

Wenn eine WDR Sub-CA Endteilnehmerzertifikate suspendiert, muss sie in ihrem CPS oder kombinierten CP/CPS den Ablauf der Suspendierung dokumentieren.

4.9.16 Maximale Sperrdauer bei Suspendierung

Eine Suspendierung von Zertifikaten findet bei der WDR RfA-CA nicht statt.

Wenn ein WDR Sub-CA Endteilnehmerzertifikate suspendiert wird, muss sie in ihrem CPS oder kombinierten CP/CPS die maximale Sperrdauer der Suspendierung dokumentiert werden.

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

Die WDR RfA-CA bietet keinen OCSP-Dienst zur Statusabfrage von Zertifikaten.

Von Seiten der WDR RfA-CA bestehen an WDR Sub-CAs keine Anforderungen an einen OCSP-Dienst zur Statusabfrage von Zertifikaten.

4.10.1 Betriebsbedingte Eigenschaften

Keine weiteren Festlegungen (s.o.).

4.10.2 Verfügbarkeit des Dienstes

Keine weiteren Festlegungen (s.o.).

4.10.3 Weitere Merkmale

Keine weiteren Festlegungen (s.o.).

4.11 Beendigung des Vertragsverhältnisses

Falls eine WDR Organisationseinheit, die eine Sub-CA betreibt, aufgelöst wird, muss der Betrieb geregelt an eine andere Organisationseinheit des WDR übergeben werden. Andernfalls wird das zugehörige CA-Zertifikat gesperrt.

Bei Beendigung des Arbeitsvertrags eines WDR Mitarbeiters oder eines externen Mitarbeiters muss sein Zertifikat gesperrt werden.

4.12 Schlüsselhinterlegung und Wiederherstellung

4.12.1 Richtlinien und Verfahren zur Schlüsselhinterlegung und Wiederherstellung

Die WDR RfA-CA bietet keine Schlüsselhinterlegung für untergeordnete CAs an.

Der WDR RfA-CA eigene Schlüssel ist auf drei Ersatz-Smartcards gesichert. Diese Ersatz-Smartcards mit den Sicherungskopien des WDR RfA-CA Schlüssels werden im Tresor 3 verwahrt. Dort liegen zu Disaster-Recovery-Zwecken auch die Sicherheitskopie der WDR RfA-CA VM und das aktuelle Backup der WDR RfA-CA Datenbank und der Log-Dateien. Die versiegelten PIN/PUK Briefe für die Ersatz-Smartcards der WDR RfA-CA und die beiden Passworthälften für die WDR RfA-CA VM befinden sich im Tresor 2 beim WDR.

Bietet eine WDR Sub-CA eine Schlüsselhinterlegung an, muss sie die Verfahren und Prozesse der Schlüsselhinterlegung in ihrem CP/CPS Dokument dokumentieren. Diese müssen der eigenen Sicherheitsrichtlinie und dem aktuellen Stand der Technik entsprechen. Es darf keine zentrale Schlüsselhinterlegung für Authentisierungs- und Signaturschlüsseln von Benutzern erfolgen, da der Zertifikatsinhaber mit diesen privaten Schlüsseln seine

Authentizität nachweist. Durch eine zentrale Schlüsselhinterlegung wären die privaten Schlüssel angreifbar.

4.12.2 Richtlinien und Verfahren zum Schutz und Wiederherstellung von Sitzungsschlüsseln

Keine weiteren Festlegungen. Es werden keine Sitzungsschlüssel verwendet.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Alle zentralen Komponenten der WDR PKI sind in einer geschützten Umgebung im Rechenzentrum des WDR untergebracht. Dort werden physikalische Sicherheitsmaßnahmen angewandt, die dem Stand der Technik entsprechen. Der Schutz der PKI-Komponenten entspricht dem anderer Serversysteme, die beim WDR im Einsatz sind.

5.1.1 Lage und Gebäude

Die Maschine der WDR RfA-CA wird nicht im Rechenzentrum beim WDR, sondern auf einem Notebook betrieben, das bei Nichtgebrauch sicher in Tresor 1 verwahrt wird. Für den Schutz des privaten Schlüssels der WDR RfA-CA werden Smartcards verwendet. Bei Nichtgebrauch wird die produktive Smartcard der WDR RfA-CA ebenfalls im Tresor 1 aufbewahrt.

Die zentralen WDR Sub-CA Komponenten sind in einer geschützten Umgebung im Rechenzentrum des WDR untergebracht. Dort werden physikalische Sicherheitsmaßnahmen angewandt, die dem Stand der Technik entsprechen. Der Schutz aller WDR PKI-Komponenten entspricht dem anderer Serversysteme, die beim WDR im Einsatz sind.

5.1.2 Zugang

Der Zugang zum Tresor 1 ist nur autorisierten Personen gestattet und ist im CP/CPS Dokument beschrieben. Der Zugang zu den WDR Sub-CA Komponenten ist ebenfalls nur autorisierten Personen gestattet. Diese sind im CP/CPS Dokument hinterlegt.

5.1.3 Strom, Heizung Klima

Die WDR RfA-CA ist nicht eingeschaltet und befindet sich in einem physikalischen Tresor 1. Daher ist dort keine Stromversorgung und Klimatisierung erforderlich.

Bei Bedarf wird diese entnommen und eingeschaltet. Die Stromversorgung und Klimatisierung erfolgt dann durch die örtlichen Gegebenheiten des Ortes an dem diese eingeschaltet wird.

5.1.4 Wassergefährdung

Wassergefährdung im physikalischen Tresor 1 entspricht dem Schutz der Serversysteme, die beim WDR im Einsatz sind. Diese Bedingungen gelten ebenfalls für die WDR Sub-CAs.

5.1.5 Brandschutz

Brandschutz im physikalischen Tresor 1 entspricht dem Schutz der Serversysteme, die beim WDR im Einsatz sind. Diese Bedingungen gelten ebenfalls für die WDR Sub-CAs.

5.1.6 Lager und Archiv

Die Datenträger mit sicherheitsrelevanten, vertraulichen Daten werden vor unberechtigten Zugriffen im Tresor auf einem externen Speichermedium geschützt aufbewahrt. Diese Bedingungen gelten ebenfalls für die WDR Sub-CAs.

5.1.7 Datenvernichtung

Bei der Entsorgung von Papierdokumenten und elektronischen Datenträgern ist sichergestellt sein, dass alle sicherheitsrelevanten, vertraulichen oder personenbezogenen Daten vernichtet sind. Diese Bedingungen gelten ebenfalls für die WDR Sub-CAs.

5.1.8 Disaster Backup

Zu Disaster-Recovery-Zwecken ist das jeweils neueste komplette System-Backup der WDR-CA, eine Sicherheitskopie der WDR-CA Schlüssel und der zugehörige Passwortbrief sicher im Tresor 3 aufbewahrt und im CP/CPS Dokument dokumentiert. Die WDR Sub-CA soll zu Disaster Zwecken täglich gesichert werden. Der private Schlüssel der Sub-CA liegt auf einer HSM und die HSM ist redundant in zwei Rechenzentren installiert.

5.2 Organisatorische Sicherheitsmaßnahmen

Alle zentralen Komponenten der WDR PKI werden im Rechenzentrum des Unternehmens durch organisatorische Sicherheitsmaßnahmen geschützt. Der organisatorische Schutz der PKI-Komponenten entspricht dem anderer Serversysteme, die beim WDR im Einsatz sind.

Auch die zentralen Komponenten der WDR Sub-CAs müssen im WDR Rechenzentrum betrieben werden.

5.2.1 Rollenkonzept

Für den Aufbau und Betrieb der WDR RfA-CA werden folgende Rollen unterschieden:

Rolle	Typ der Rolle	Mindest-Anzahl der Personen	Aufgabe
Lokaler Administrator der WDR RfA-CA VM	Betriebssystem	2 + 2 Vertreter	Administration des Betriebssystems der WDR RfA-CA VM Hinterlegen die ihnen bekannten Passworthälften separat im elektronischen Passwortsafe des WDR.
WDR RfA-CA Administrator	PKI	2 + 2 Vertreter	Konfiguriert und wartet die WDR RfA-CA. Ist auch verantwortlich für die Zertifikatsausstellung und ggf. -sperrung von Sub-CAs. Übernimmt die Veröffentlichung der WDR RfA-CA Sperrliste. Kennt jeweils einen Teil der PIN der CA-Smartcard. Hinterlegen die ihnen bekannten PIN- und PUK-Teile separat im elektronischen Passwortsafe des WDR.

Tresorverwalter für Tresor 1	Schließ-regelung	1 + 1 Vertreter	Zugriff auf den Tresor 1 beim WDR. Dort werden verwahrt: • Notebook mit der virtuellen Maschine der WDR RfA-CA • Jeweils separat versiegelte PIN- und PUK-Briefe der produktiven WDR RfA-CA Smartcard
Tresorverwalter für Tresor 2	Schließ-regelung	1	Zugriff auf den Tresor 2 beim WDR. Dort werden verwahrt: • Produktive CA-Smartcard der WDR RfA-CA • Versiegelte Umschläge mit den Passworthälften des lokalen System Administrators der WDR RfA-CA VM • Jeweils separat versiegelte PIN- und PUK-Briefe der Ersatz-Smartcards der WDR RfA-CA
Tresorverwalter für Tresor 3	Schließ-regelung	1	Zugriff auf den Tresor 3 beim WDR. Dort werden als Disaster Recovery Backup verwahrt: • Ersatz-Smartcards der WDR RfA-CA • Backup der virtuellen Maschine der WDR RfA-CA auf einem optischen Speichermedium • Backup der WDR RfA-CA Datenbank und Log-Dateien auf einem optischen Speichermedium

Tabelle 1: Rollen für Aufbau und Betrieb der WDR RfA-CA

Für den Aufbau und Betrieb einer WDR Sub-CA sind geeignete Rollen definiert und umgesetzt. Diese werden von der WDR Sub-CA in ihrem CPS oder kombinierten CP/CPS dokumentiert.

5.2.2 Anzahl involvierter Personen pro Aufgabe

Für die beiden Rollen „Lokaler Administrator der WDR RfA-CA VM“ und „WDR RfA-CA Administrator“ sind jeweils mindestens zwei Personen gleichzeitig erforderlich, um ein Vier-Augen-Prinzip umzusetzen.

Die beiden Rollen „Lokaler Administrator der WDR RfA-CA VM“ und „WDR RfA-CA Administrator” sind konzeptionell getrennt, können aber von den gleichen Personen übernommen werden, d. h. die Personen, die als „Lokaler Administrator der WDR RfA-CA VM“ auftreten, können auch als „WDR RfA-CA Administrator“ agieren, sofern die CA-Administration nicht aus anderen Gründen von der Betriebssystem-Administration getrennt werden soll.

Für die Rollen einer WDR Sub-CA ist kein Vier-Augen-Prinzip erforderlich. Es sei denn, die WDR Sub-CA bietet die Wiederherstellung von Verschlüsselungsschlüsseln (Key Recovery) an; hierfür ist ein Vier-Augen-Prinzip erforderlich.

5.2.3 Identifizierung und Authentifizierung jeder Rolle

Alle Rollen der WDR RfA-CA verwenden Benutzername und Passwort zur Authentifizierung.

Zur Authentifizierung bei allen Rollen einer WDR Sub-CA genügt ebenfalls eine Ein-Faktor-Authentifizierung, wie bspw. Benutzername und Passwort.

5.2.4 Rollen, die eine Aufgabentrennung erfordern

Die Rolle eines Tresorverwalters darf nicht in Personalunion mit der Rolle eines anderen Tresorverwalters und auch nicht mit einer der Rollen „Lokaler Administrator der WDR RfA-CA VM“ oder „WDR RfA-CA Administrator“ übernommen werden. Damit soll die logische Zugriffsberechtigung auf die WDR RfA-CA von der physischen Zugriffsberechtigung auf das Notebook mit der WDR RfA-CA VM getrennt werden und keine Rolle alleine Zugriff und Zugang zu der eingelagerten WDR RfA-CA haben.

Für Installation, Konfiguration und Betrieb der WDR Sub-CA ist für keine der Rollen eine Aufgabentrennung erforderlich.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an Mitarbeiter

Die PKI-Administratoren beim WDR sind feste Mitarbeiter des WDR. Sie sind zur Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet. Sie verfügen über ausreichende Fachkunde, um die WDR RfA-CA sicher zu betreiben.

Auch die CA-Administratoren einer WDR Sub-CA müssen den Stand der Technik und die Best Practices im Bereich Zertifikatsinfrastruktur kennen.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Für die CA-Administratoren der WDR RfA-CA („Lokaler Administrator der WDR RfA-CA VM“ und „WDR RfA-CA Administrator“) wird keine Sicherheitsüberprüfung durchgeführt.

Auch für die CA-Administratoren einer WDR Sub-CA ist keine Sicherheitsüberprüfung erforderlich.

5.3.3 Anforderungen an Schulungen

Keine weiteren Festlegungen. Es bestehen keine Anforderungen an Schulungen.

5.3.4 Häufigkeit und Anforderungen an Fortbildungen

Alle PKI-Administratoren des WDR besuchen mindestens alle zwei Jahre eine PKI-Schulung oder halten sich auf andere Weise über den Stand der Technik und die Best Practices im Bereich PKI auf dem Laufenden.

5.3.5 Häufigkeit und Ablauf von Arbeitsplatzwechseln

Keine weiteren Festlegungen. Es findet kein regelmäßiger Arbeitsplatzwechsel für PKI-Administratoren statt.

5.3.6 Sanktionen für unerlaubte Handlungen

Keine weiteren Festlegungen. Die PKI-Administratoren der WDR RfA-CA unterliegen – wie alle Mitarbeiter des WDR - den arbeitsrechtlich zulässigen Sanktionsmöglichkeiten.

5.3.7 Anforderungen an freie Mitarbeiter

Keine weiteren Festlegungen. Es gibt keine zusätzlichen Anforderungen an freie Mitarbeiter.

5.3.8 Dokumentation für Mitarbeiter

Alle PKI-Administratoren beim WDR erhalten die Mindestanforderungen der Rundfunk-Root-CA und dieses Dokument zur Kenntnis.

5.4 Überwachungsmaßnahmen

Alle sicherheitsrelevanten Ereignisse der WDR RfA-CA und der WDR Sub-CAs werden in Log-Dateien protokolliert. Für Nutzer der WDR PKI besteht kein Anspruch, entsprechende Daten einzusehen.

5.4.1 Überwachte Ereignisse

Zu den sicherheitsrelevanten Ereignisse der WDR RfA-CA bzw. WDR Sub-CA zählen z. B.:

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

5.4.2 Häufigkeit der Protokollanalyse

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

Die Log-Daten einer WDR Sub-CA sind kontinuierlich auf sicherheitsrelevante Einträge zu überprüfen. Darüber hinaus wird im Fall eines begründeten Verdachts auf Missbrauch der WDR Sub-CA von den PKI-Administratoren eine anlassbezogene Auswertung der Log-Daten der WDR Sub-CA nach Vorgabe der IT-Sicherheitsordnung des WDR vorgenommen.

5.4.3 Aufbewahrungsfrist für Protokolldaten

Das Ereignisprotokoll der WDR RfA-CA wird mindestens 7 Tage aufbewahrt.

Die Aufbewahrungsfrist für Protokolldaten einer WDR Sub-CA sind ebenfalls mindestens 7 Tage aufzubewahren und sind in ihrem CPS oder kombinierten CP/CPS zu dokumentieren.

5.4.4 Schutz von Protokolldaten

Die Protokolldaten der WDR RfA-CA sind über die Zugriffskontrolle des Betriebssystems gegen unberechtigten Zugriff, Löschung und Manipulation geschützt.

Außerdem werden bei der WDR RfA-CA werden die Protokolldaten nach jeder sicherheitsrelevanten Aktion auf ein optisches Speichermedium gebrannt und dem zuständigen Tresorverwalter übergeben, der dieses im Tresor 3 beim WDR verwahrt.

Die Protokolldaten einer WDR Sub-CA müssen ebenfalls gegen unberechtigten Zugriff, Löschung und Manipulation geschützt werden.

5.4.5 Backup der Protokolldaten

Bei der WDR RfA-CA werden die Protokolldaten nach jeder sicherheitsrelevanten Aktion von den beiden PKI-Administratoren der WDR RfA-CA auf ein optisches Speichermedium gebrannt, das im Tresor 3 beim WDR verwahrt wird.

Bei den WDR Sub-CAs sind die Protokolldaten im Rahmen des normalen Serverbetriebs zu sichern.

5.4.6 Überwachungssystem

Keine weiteren Festlegungen. Für die Protokolldaten der WDR RfA-CA wird kein Überwachungssystem eingesetzt, da die CA offline betrieben wird.

Die Protokolldaten einer WDR Sub-CA sollten automatisiert überwacht werden. Die Beschreibung der Überwachung sollte von der WDR Sub-CA in ihrem CPS oder kombinierten CP/CPS dokumentiert werden.

5.4.7 Benachrichtigung bei schwerwiegenden Ereignissen

Keine weiteren Festlegungen. Siehe Kapitel 5.4.2

5.4.8 Schwachstellenanalyse

Bei der WDR RfA-CA findet keine kontinuierliche Schwachstellenanalyse statt. Die Software der WDR RfA-CA wird nicht im Patch-Management des WDR aufgenommen. Auftretende Schwachstellen in der Software der WDR RfA-CA werden nicht behoben, da die WDR RfA-CA eine offline-CA ist und bei Nichtgebrauch sicher in einem Tresor beim WDR verwahrt wird.

Spätestens mit der Inbetriebnahme einer WDR Sub-CA ist die Software der WDR Sub-CA in das Patch-Management des WDR aufzunehmen. Schwachstellen bei den eingesetzten Systemen sind nach Bekanntwerden der Schwachstelle und Vorliegen eines Patches umgehend zu schließen.

5.5 Archivierung

5.5.1 Archivierte Daten

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

- Sicherheitskopien des WDR RfA-CA Schlüssels auf drei Ersatzkarten
- Passwort-Briefe mit den beiden Hälften der PIN für die produktive Smartcard und die Ersatzkarten der WDR RfA-CA
- Passwort-Briefe mit den beiden Hälften der PUK für die produktive Smartcard und die Ersatzkarten der WDR RfA-CA
- Passwort-Briefe mit den beiden Hälften des Passworts für das lokale Administratorkonto der WDR RfA-CA
- Backup der virtuellen Maschine der WDR RfA-CA auf einem optischen Speichermedium
- Backup der WDR RfA-CA Datenbank und Log-Dateien auf einem optischen Speicher-medium
- Zertifikats- und Sperranträge an die WDR RfA-CA

Art und Umfang der Daten, die von einer WDR Sub-CA aufbewahrt werden müssen:

- Sicherungskopie des WDR Sub-CA-Schlüssels
- Passwort-Brief mit dem Passwort für den archivierten WDR Sub-CA Schlüssel
- Über die Archivierung von Zertifikats-, Sperranträgen, Log-Dateien, etc. entscheidet jede WDR Sub-CA abhängig von den Anforderungen der von ihr unterstützten Anwendungen.

5.5.2 Aufbewahrungsfrist für archivierte Daten

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

Die gleiche Anforderung gilt für WDR Sub-CAs.

5.5.3 Schutz der Archive

Die Ersatzkarten mit den Sicherungskopien des WDR RfA-CA Schlüssels sowie die Passwortbriefe werden vor unberechtigtem Zugriff geschützt in verschiedenen Tresoren des WDR so aufbewahrt, dass keine Smartcard mit ihrer zugehörigen PIN/PUK im gleichen Tresor liegt. Auch das Notebook mit der virtuellen Maschine der WDR RfA-CA, das Backup der virtuellen Maschine der WDR RfA-CA und das Passwort für das lokale Administratorkonto werden in getrennten Tresoren verwahrt.

Die Sicherungskopie eines WDR Sub-CA Schlüssels sowie das Passwort für die Sicherungskopie sollen ebenfalls vor unberechtigtem Zugriff geschützt verwahrt.

5.5.4 Datensicherung des Archivs

Für die im Tresor aufbewahrten Daten ist keine elektronische Datensicherung erforderlich.

5.5.5 Anforderungen an Zeitstempel

Es bestehen keine Anforderungen an Zeitstempel, da die aufzubewahrenden Daten nicht in elektronischer Form vorliegen[2].

5.5.6 Archivierungssystem

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

5.5.7 Prozeduren für Abruf und Überprüfung archivierter Daten

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

5.6 Schlüsselwechsel der Zertifizierungsstelle

Der private Schlüssel der WDR RfA-CA wird nur so lange zum Ausstellen von Sub-CA-Zertifikaten eingesetzt, wie die Gültigkeit der untergeordneten Zertifikate noch innerhalb des Gültigkeitsrahmens des WDR RfA-CA-Zertifikats liegt (siehe auch Kapitel 6.3.2).

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

Die gleichen Anforderungen bzgl. Schlüsselwechsel gelten für WDR Sub-CAs.

5.7 Kompromittierung und Wiederherstellung

5.7.1 Vorgehen bei Sicherheitsvorfällen und Kompromittierung

Falls im Laufe der Gültigkeitsdauer des WDR RfA-CA Zertifikats die verwendeten Kryptoverfahren bzw. Schlüssellängen (siehe Kapitel 6.1 und 7.1) nicht mehr als hinreichend sicher zu betrachten sind, wird gemäß der beim WDR definierten Behandlung von IT-Sicherheitsvorfällen verfahren und die CA Steuerungsgruppe zu informieren.

Bei ungeeigneten Kryptoverfahren oder nicht ausreichenden Schlüssellängen müssen das Zertifikat der WDR RfA-CA und alle von ihr erstellten Sub-CA Zertifikate gesperrt und die WDR RfA-CA durch eine neue CA ersetzt werden. Die Außerbetriebnahme der bestehenden WDR RfA-CA wird in Abschnitt 5.8 beschrieben. Beim Aufbau einer neuen WDR RfA-CA ist das gesamte Schlüsselmaterial der CA neu zu generieren und ein neues Zertifikat bei der

[2] Zeitstempel dienen zum Erhalt der Sicherheitseigenschaften von signierten elektronischen Dokumenten bei Langzeitarchivierung.

Rundfunk-Root-CA zu beantragen. Anschließend müssen alle Sub-CA Zertifikate von der WDR RfA-CA neu ausgestellt werden.

Die Anforderungen bzgl. des Vorgehens bei Sicherheitsvorfällen und Kompromittierung gelten für WDR Sub-CAs gleichermaßen.

5.7.2 Betriebsmittel, Software und/oder Daten sind korrumpiert

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

Im Fall korrumpierter Software oder Daten wird die Sicherheitskopie der virtuellen Maschine der WDR RfA-CA mit dem Backup der WDR RfA-CA Datenbank und Log-Dateien auf ein Notebook aufgespielt und zukünftig verwendet. In diesem Fall werden unmittelbar nach der Inbetriebnahme so viele Sperrlisten erstellt, bis die CRLNumber (siehe Abschnitt 7.2.2) größer ist, als diejenige in der letzten veröffentlichten CRL der WDR RfA-CA.

Auch für WDR Sub-CAs gilt die Anforderung: Im Verdachtsfall von kompromittierter Software oder Daten sind die Daten aus einer unkompromittierten Datensicherung zurück zu spielen.

5.7.3 Kompromittierung des privaten Schlüssels

Bei hinreichendem Verdacht auf eine Kompromittierung des privaten Schlüssels der WDR RfA-CA wird von den PKI-Administratoren eine anlassbezogene Auswertung des Vorfalls nach Vorgabe der IT-Sicherheitsordnung des WDR vorgenommen. Bei einer Kompromittierung muss das Zertifikat der WDR RfA-CA und alle von ihr erstellten Sub-CA Zertifikate gesperrt und die WDR RfA-CA durch eine neue CA ersetzt werden. Die Außerbetriebnahme der bestehenden WDR RfA-CA wird in Abschnitt 5.8 beschrieben.
Beim Aufbau einer neuen WDR RfA-CA ist das gesamte Schlüsselmaterial der CA neu zu generieren und ein neues Zertifikat bei der Rundfunk-Root-CA zu beantragen. Anschließend müssen alle Sub-CA Zertifikate von der WDR RfA-CA neu ausgestellt werden.

Auch für WDR Sub-CAs gilt: Bei hinreichendem Verdacht auf eine Kompromittierung des privaten Schlüssels einer WDR Sub-CA ist unverzüglich die Sperrung des WDR Sub-CA Zertifikats bei der WDR RfA-CA zu beantragen und danach neue Schlüssel zu erzeugen und ein neues Zertifikat zu beantragen.

5.7.4 Wiederaufnahme des Betriebs nach einem Notfall

Die Wiederaufnahme des Betriebs nach einem Katastrophenfall entspricht den in den vorangegangen Kapiteln 5.7.1, 5.7.2. und 5.7.3 beschriebenen Vorgehensweisen.

5.8 Einstellung des Betriebs

Wenn die WDR RfA-CA ihren Betrieb einstellt, muss sie einen Sperrantrag bei der Rundfunk-Root-CA stellen. Mit der Sperrung des WDR RfA-CA Zertifikats werden automatisch auch alle untergeordneten Zertifikate ungültig. Alle von der WDR RfA-CA ausgestellten Zertifikate, die noch gültig sind, werden gesperrt und anschließend eine letzte Sperrliste ausgestellt und veröffentlicht, die bis zum Ende der Laufzeit des WDR RfA-CA Zertifikats gültig ist. Abschließend werden die produktive Smartcard und alle Ersatzkarten der WDR RfA-CA vernichtet (siehe Abschnitt 6.2.10).

Wenn eine WDR Sub-CA ihren Betrieb einstellt, muss sichergestellt werden, dass die von ihr ausgestellten Zertifikate nicht mehr verwendet werden können, da sie nicht mehr gesperrt werden können. Außerdem ist dafür zu sorgen, dass der private Schlüssel der WDR Sub-CA nicht missbräuchlich verwendet werden kann.

6 Technische Sicherheitsmaßnahmen

6.1 Schlüsselerzeugung und Installation

6.1.1 Schlüsselerzeugung

Bei der Key-Zeremonie der WDR RfA-CA wurden unter Zeugen die Schlüssel der WDR RfA-CA erzeugt und in eine produktive CA-Smartcard sowie die drei Ersatz-Smartcards importiert. Anschließend wurden die Schlüssel von der Festplatte sicher gelöscht.

Schlüssel untergeordneter Zertifizierungsstellen müssen dezentral von der betreffenden WDR Sub-CA erzeugt werden.

6.1.2 Übermittlung privater Schlüssel an Zertifikatsinhaber

Da die Schlüssel untergeordneter Zertifizierungsstellen dezentral von der betreffenden WDR Sub-CA selbst erzeugt werden, ist keine Übermittlung notwendig.

Abhängig davon, ob eine WDR Sub-CA eine zentrale Schlüsselerzeugung anbietet oder die Endanwender ihre Schlüssel selber erzeugen müssen, ist eine Übermittlung des privaten Schlüssels von einer WDR Sub-CA an einen Endanwender erforderlich. Die Übermittlung privater Schlüssel muss im CPS oder kombinierten CP/CPS der WDR Sub-CA dokumentiert werden.

6.1.3 Übermittlung öffentlicher Schlüssel an Zertifikatsaussteller

Zu zertifizierende öffentliche Schlüssel von WDR Sub-CAs werden in Form eines signierten Zertifikatsantrags (Certificate Signing Request, CSR) auf vertrauenswürdigem Wege an die PKI-Administratoren der WDR RfA-CA übermittelt. Zulässig ist die Beantragung via E-Mail mit Rückruf an die vorab angegebene Telefonnummer des PKI-Ansprechpartners oder seines Vertreters 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.

Abhängig davon, ob eine WDR Sub-CA eine zentrale Schlüsselerzeugung anbietet oder die Endanwender ihre Schlüssel selber erzeugen müssen, ist eine Übermittlung des öffentlichen Schlüssels vom Endanwender an eine WDR Sub-CA erforderlich. Die Übermittlung öffentlicher Schlüssel muss im CPS oder kombinierten CP/CPS der WDR Sub-CA dokumentiert werden.

6.1.4 Verteilung des öffentlichen CA-Schlüssels an Zertifikatsprüfer (Relying Parties)

Das CA-Zertifikat mit dem öffentlichen Schlüssel der WDR RfA-CA wird im Active Directory, im Daten-CN und im Internet bereit gestellt (siehe Kapitel 2.1). Die URLs, von denen das CA-Zertifikat der WDR RfA-CA abgerufen werden kann, werden in einer Zertifikatserweiterung in den ausgestellten WDR Sub-CA-Zertifikaten vermerkt (siehe Kapitel 7.1.2).

WDR Sub-CAs müssen ihr CA-Zertifikat, das von der WDR RfA-CA ausgestellt wurde, im Active Directory und bei Bedarf auch im Daten-CN und im Internet bereitstellen. Die URLs, von denen das WDR Sub-CA Zertifikat abgerufen werden kann, sollten in einer Zertifikatserweiterung in den ausgestellten Endanwenderzertifikaten vermerkt werden.

6.1.5 Schlüssellängen

Die WDR RfA-CA nutzt das RSA Kryptoverfahren mit einer Schlüssellänge von 4096 Bit.

Die Schlüsselpaare der WDR Sub-CAs und der Endnutzer oder -systeme müssen mindestens 2048 Bit lang sein. Es werden keine bestehenden Schlüsselpaare mit kürzeren Schlüssellängen für Endnutzer oder -systeme verwendet.

6.1.6 Erzeugung der Public Key Parameter und Qualitätssicherung

Die Schlüssel der WDR RfA-CA wurden mittels OpenSSL erzeugt. Das Prüfverfahren und die Anforderungen zur Prüfung des RSA Algorithmus inklusive der Schlüsselgenerierung sind vom NIST spezifiziert. Die Qualität der erzeugten Public Key Parameter mittels OpenSSL entsprechen diesen Anforderungen aus FIPS 140-2[3].

Die Erzeugung der WDR Sub-CA Schlüssel muss im CPS oder kombinierten CP/CPS der WDR Sub-CA dokumentiert werden.

6.1.7 Schlüsselverwendungszwecke

Das CA-Zertifikat der WDR RfA-CA enthält eine Schlüsselverwendungserweiterung (englisch: KeyUsage Extension) mit den Einträgen Zertifikatssignatur und Sperrlistensignatur (englisch: keyCertSign, cRLSign), d. h. dieses Zertifikat kann zur Unterzeichnung von Zertifikaten und Sperrlisten verwendet werden.

Alle von der WDR RfA-CA ausgestellten Zertifikate für weitere untergeordnete WDR Sub-CAs sowie die zugehörigen privaten Schlüssel dürfen nur zu den in den Zertifikaten spezifizierten Verwendungszwecken eingesetzt werden (KeyUsage Erweiterung, siehe Kapitel 7.1.2).

Zertifikatsprüfer (Relying Parties) müssen diese Schlüsselverwendungszwecke prüfen, bevor sie das Zertifikat verwenden.

6.2 Schutz privater Schlüssel und Einsatz kryptographischer Module

6.2.1 Standard kryptographischer Module

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

Einsatz und Standard eines kryptographischen Moduls zur Speicherung eines WDR Sub-CA Schlüssels müssen im CPS oder kombinierten CP/CPS der WDR Sub-CA dokumentiert werden.

6.2.2 Aufteilung privater Schlüssel auf mehrere Personen

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

Die Aktivierung des privaten Schlüssels einer WDR Sub-CA erfordert kein Vier-Augen-Prinzip.

6.2.3 Hinterlegung privater Schlüssel

Der private Schlüssel der WDR RfA-CA wird nicht hinterlegt, d.h. es findet kein Key Escrow statt.

Auch die privaten Schlüssel einer WDR Sub-CA und deren Endteilnehmer dürfen nicht hinterlegt werden.

---

3 https://www.openssl.org/docs/fips/fipsvalidation.html

6.2.4 Backup privater Schlüssel

Der private Schlüssel der WDR RfA-CA wurde in drei Ersatzkarten importiert. Als Ersatzkarten wurde der gleiche Typ Smartcard wie für die produktive Smartcard verwendet, der nach Common Criteria EAL4+ zertifiziert ist.

Das Backup eines privaten WDR Sub-CA Schlüssels muss im CPS oder kombinierten CP/CPS der WDR Sub-CA dokumentiert werden.

6.2.5 Archivierung privater Schlüssel

Die im vorigen Abschnitt genannten Ersatzkarten werden in einem separaten Tresor beim WDR aufbewahrt.

Die Archivierung eines privaten WDR Sub-CA Schlüssels muss im CPS oder kombinierten CP/CPS der WDR Sub-CA dokumentiert werden.

6.2.6 Transfer privater Schlüssel in oder aus einem kryptographischen Modul

Der private Schlüssel der WDR RfA-CA wurde ausschließlich in die produktive Smartcard und drei Ersatzkarten importiert.

Der Transfer eines privaten WDR Sub-CA Schlüssels in oder aus einem kryptographischen Modul muss im CPS oder kombinierten CP/CPS der WDR Sub-CA dokumentiert werden.

6.2.7 Speicherung privater Schlüssel in einem kryptographischen Modul

Der private Schlüssel der WDR RfA-CA wird in einer Smartcard gespeichert.

Die privaten Schlüssel von WDR Sub-CAs, Endanwendern und Systemen können sowohl auf Smartcard oder HSM als auch in Software gespeichert werden.

6.2.8 Aktivierung privater Schlüssel

Die Aktivierung des privaten Schlüssels der WDR RfA-CA ist nur durch PIN-Eingabe im Vier-Augen-Prinzip möglich.

Die privaten Schlüssel der Endanwender der WDR SUB-Ca müssen durch ein geeignetes Passwort vor unautorisiertem Zugriff geschützt werden.

Der Zugriff auf den privaten Schlüssel von Systemen der WDR Sub-CA muss hingegen nicht zwingend durch ein Passwort gesichert sein. Dafür muss aber der Zugriff auf die Systeme hinreichend gesichert werden.

6.2.9 Deaktivierung privater Schlüssel

Software-erzeugter Schlüssel der RfA-CA wird im Rahmen der Key-Zeremonie auf SmartCards übertragen und sicher gelöscht.

Der private Schlüssel der WDR RfA-CA bleibt nur so lange aktiv, wie der Server der WDR RfA-CA in Betrieb ist und neue Sub-CA-Zertifikate oder Sperrlisten erstellt werden. Danach wird er unverzüglich durch Ziehen der Smartcard aus dem Kartenleser oder durch Beendigung der Zertifikatsdienste wieder deaktiviert.

Der private Schlüssel einer WDR Sub-CA darf durchgehend aktiviert bleiben, solange der Server der WDR Sub-CA in Betrieb ist.

6.2.10 Vernichtung privater Schlüssel

Sollte es nötig werden, den privaten Schlüssel der WDR RfA-CA zu löschen, so werden die produktive Smartcard und die drei Ersatzkarten physisch zerstört.

Wird der private Schlüssel einer WDR Sub-CA nicht mehr benötigt, muss auch dieser sicher gelöscht werden.

6.2.11 Güte kryptographischer Module

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

Anforderungen an die Güte kryptographischer Module für WDR Sub-CAs müssen im CPS oder kombinierten CP/CPS der WDR Sub-CA dokumentiert werden.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Keine weiteren Festlegungen. Öffentliche Schlüssel werden nicht archiviert.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Das von der Rundfunk-Root-CA ausgestellte RfA-CA Zertifikat für den WDR ist ab dem Ausstellungszeitpunkt 20 Jahre, d. h. bis 2035 gültig. Der zugehörige private Schlüssel wird aber nur für 10 Jahre zur Ausstellung untergeordneter Sub-CA Zertifikate genutzt. In den letzten zehn Jahren seiner Laufzeit wird er nicht mehr zur Ausstellung weiterer Sub-CA Zertifikate genutzt, da diese Sub-CA Zertifikate ab diesem Zeitpunkt keine 10 Jahre mehr gültig sein können.

Das Zertifikat einer WDR Sub-CA ist 10 Jahre gültig. Der Verwendungszeitraum des privaten Schlüssels einer WDR Sub-CA ist von der Laufzeit der auszustellenden Endteilnehmer-zertifikate abhängig. Die Laufzeit der Endteilnehmerzertifikate und damit verbunden der Verwendungszeitraum des privaten Schlüssels einer WDR Sub-CA müssen im CPS oder kombinierten CP/CPS der WDR Sub-CA dokumentiert werden.

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation der Aktivierungsdaten

Die PIN zur Aktivierung des privaten Schlüssels der WDR RfA-CA ist vier Zeichen lang. Sie wurde von den beiden PKI-Administratoren während der Key-Zeremonie der WDR RfA-CA festgelegt.

Die Erzeugung und Installation der Aktivierungsdaten einer WDR Sub-CA sind im CPS oder kombinierten CP/CPS der WDR Sub-CA dokumentiert. Diese entsprechen den WDR Schutzmechanismen und müssen im CPS oder kombinierten CP/CPS der WDR Sub-CA dokumentiert werden.

6.4.2 Schutz der Aktivierungsdaten

Zur Wahrung des Vier-Augen-Prinzips ist die PIN auf die beiden PKI-Administratoren der WDR RfA-CA aufgeteilt. Die beiden Hälften der PIN werden in je einem versiegelten Umschlag in Tresor 1 beim WDR aufbewahrt.

Schutzmechanismen zu den Aktivierungsdaten einer WDR Sub-CA müssen im CPS oder kombinierten CP/CPS der WDR Sub-CA dokumentiert werden.

6.4.3 Weitere Aspekte

Keine weiteren Festlegungen.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Für die zentralen Komponenten der WDR RfA-CA gelten dieselben IT-Sicherheitsmaßnahmen wie für die anderen Serversysteme vom WDR.

Die WDR RfA-CA läuft auf einem dafür vorgesehenen Notebook. Auf dem Notebook sind alle aktuellen Patches, ein aktueller Virenscanner und der Treiber für den Smarcardleser installiert. hat keine Netzwerkschnittstelle. Sie ist keinem AD angeschlossen. Die WDR Root-CA wird im Stand-alone Modus zu betrieben. Bei Nicht-Gebrauch wird das Notebook im Tresor 1 beim WDR aufbewahrt.

Die WDR RfA-CA wird durch geeigneter Benutzerauthentisierung und Zugriffskontrolle vor unberechtigten Zugriffen geschützt. Sowohl der lokale System Administrator als auch der WDR RfA-CA Administrator haben ein Passwort bestehend aus 12 Zeichen. Beide Passwörter sind in zwei Teile geteilt. Weitere Benutzer haben keinen Zugriff auf die VM.

Für die zentralen Komponenten einer WDR Sub-CA gelten dieselben IT-Sicherheitsanforderungen wie für die anderen Serversysteme beim WDR. Nicht benötigte Dienste werden deaktiviert oder nicht installiert. Das Betriebsystem wird nach WDR Sicherheitsvorgaben gehärtet .

Diese Vorgaben müssen in im kombiniertem CP/CPS Dokument der WDR SUB-CA dokumentiert sein.

6.5.2 Beurteilung von Computersicherheit

Keine weiteren Festlegungen. Für den Computer gibt es keine Gütesiegel in Form von Zertifikaten wie bspw. eine CC-Evaluierung und Bestätigung.

Auch für eine WDR Sub-CA besteht keine Anforderung nach einer Beurteilung der Computersicherheit.

6.6 Technische Maßnahmen im Lebenszyklus

6.6.1 Maßnahmen der Systementwicklung

Es findet keine Entwicklung statt.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

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

Spätestens mit der Inbetriebnahme einer WDR Sub-CA ist die Software der WDR Sub-CA in das Patch-Management des WDR aufzunehmen. Schwachstellen bei den eingesetzten Systemen sind nach Bekanntwerden der Schwachstelle und Vorliegen eines Patches umgehend zu schließen.

6.6.3 Lebenszyklus der Sicherheitsmaßnahmen

Keine weiteren Festlegungen. Die WDR RfA-CA wird auf einem offline Rechner betrieben, daher gibt es keinen Lebenszyklus der Sicherheitsmaßnahmen.

Für den Server der WDR Sub-CA gelten die gleichen Anforderung nach einem Lebenszyklus der Sicherheitsmaßnahmen wie für alle anderen Serversysteme beim WDR auch.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Die VM der WDR RfA-CA wird auf einem Notebook betrieben, das während des Betriebs der WDR RfA-CA nicht im Netzwerk des WDR hängt.

Der Server einer WDR Sub-CA muss geeignet vor Zugriffen von außen geschützt sein. Sämtliche nicht benötigten Netzdienste müssen deaktiviert werden.

6.8 Zeitstempel

Innerhalb der WDR PKI wird kein Zeitstempeldienst betrieben.

7 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen

7.1 Zertifikatsprofil

7.1.1 Versionsnummer

Es werden X.509 Zertifikate in Version 3 verwendet, d.h. die Versionsnummer im Zertifikat ist auf den Wert 2 gesetzt.

Die gleichen Anforderungen/Regelungen gelten für WDR Sub-CAs sind im kombiniertem CP/CPS Dokument zu dokumentieren.

7.1.2 Zertifikatserweiterungen

In den Zertifikaten für untergeordnete WDR Sub-CAs sind folgende Zertifikatserweiterungen enthalten:

- BasicConstraints (Basiseinschränkungen)
- ExtendedKeyUsage (Schlüsselverwendung)
- CRLDistributionPoints (Sperrlisten-Verteilungspunkte)
- AuthorityKeyIdentifier (Stellenschlüsselkennung)
- SubjectKeyIdentifier (Schlüsselkennung des Antragstellers)

Die Erweiterungen BasicConstraints und KeyUsage werden als kritisch, alle anderen als nicht-kritisch markiert. Optional können außerdem weitere nicht kritische Zertifikats-erweiterungen in den RfA-CA-Zertifikaten ergänzt werden.

In den Zertifikaten für Endanwender und Systeme müssen mindestens folgende Zertifikatserweiterungen enthalten sein:

- ExtendedKeyUsage (Schlüsselverwendung)
- CRLDistributionPoints (Sperrlisten-Verteilungspunkte)
- AuthorityKeyIdentifier (Stellenschlüsselkennung)

Die KeyUsage muss als kritisch, alle anderen als nicht-kritisch markiert werden. Optional dürfen außerdem eine kritische *BasicConstraints*-Erweiterung und weitere nicht kritische Zertifikatserweiterungen in den Zertifikaten für Endanwender und Systeme ergänzt werden, wie bspw. AuthorityInfoAccess, ExtendedKeyUsage.

Um WLAN-Clientzertifikate RFA-übergreifend einheitlich zu kennzeichnen und sie so von anderen Client-Authentisierungszertifikaten wie bspw. VPN-Zertifikaten unterscheiden zu können, muss in allen WLAN-Clientzertifikaten (Maschinenzertifikaten) ein einheitlicher ExtendedKeyUsage -Identifier enthalten sein:

- ExtendedKeyUsage : 1.3.6.1.4.1.42638.2.1

Die ExtendedKeyUsage Erweiterung soll als nicht-kritisch markiert werden.

Zusätzlich sollen in WLAN-Benutzerzertifikaten die E-Mail Adresse und der UPN des Benutzers als weitere Attribute zum Abgleich von Authentifizierungsinformationen stehen.

- SubjectAltName: E-Mail Adresse und UPN des Benutzers

Die SubjectAltName Erweiterung muss als nicht-kritisch markiert werden.

Die gleichen Anforderungen/Regelungen gelten für WDR Sub-CAs sind im kombiniertem CP/CPS Dokument dokumentiert.

7.1.3 Algorithmus Bezeichner

Es wird der Signaturalgorithmus „sha256WithRSAEncryption“ verwendet. Es gelten die gleichen Regelungen in den WDR Sub-CAs und sind im kombiniertem CP/CPS Dokument dokumentiert.

7.1.4 Namensformen

Siehe Kapitel 3.1.4.

7.1.5 Namensbeschränkungen

Es werden keine Namensbeschränkungen (englisch: Name Constraints) verwendet.

7.1.6 Bezeichner für Zertifizierungsrichtlinien

WLAN-Clientzertifikate (Benutzer- und Maschinenzertifikaten) müssen einen einheitlichen Certificate Policy-Identifier enthalten Siehe Abschnitt 7.1.2.

7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkungen

Es werden keine Beschränkungen für Sicherheitsrichtlinien (englisch: Policy Constraints) verwendet.

7.1.8 Syntax und Semantik von Policy Qualifiern

Keine weiteren Festlegungen. Es gibt keine Anforderungen an die in der CertificatePolices Erweiterung optional verwendbaren Policy Qualifier.

7.1.9 Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien

Keine weiteren Festlegungen. In der gesamten Rundfunk-PKI dürfen keine kritischen CertificatePolices Erweiterungen verwendet werden. Wenn eine CertificatePolices Erweiterung in einem Zertifikat eingetragen wird, so ist diese immer als unkritisch zu kennzeichnen.

7.2 Sperrlistenprofil

7.2.1 Versionsnummer

Es werden X.509 Sperrlisten in Version 2 verwendet, d.h. die Versionsnummer der Sperrliste ist auf den Wert 1 gesetzt. Es gelten die gleichen Regelungen in den WDR Sub-CAs und sind im kombiniertem CP/CPS Dokument dokumentiert.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

In den Sperrlisten der WDR RfA-CA sind mindestens folgende Erweiterungen enthalten:

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

Diese Sperrlistenerweiterungen werden alle als nicht kritisch markiert. Optional können weitere nicht kritische Erweiterungen in den Sperrlisten ergänzt werden.

Es gelten die gleichen Regelungen in den WDR Sub-CAs und sind im kombiniertem CP/CPS Dokument dokumentiert.

7.3 OCSP Profil

7.3.1 Versionsnummer

Die WDR RfA-CA bietet keinen Online-Auskunftsdienst zum Status von Zertifikaten an.

7.3.2 OCSP Erweiterungen

Die WDR RfA-CA bietet keinen Online-Auskunftsdienst zum Status von Zertifikaten an.

8 Konformitätsprüfung (Audit)

Eine Evaluierung der WDR RfA-CA nach Common Criteria, ITSEC, FIPS PUB 140.2 oder nach einem ähnlichen Standard ist nicht vorgesehen.

8.1 Häufigkeit und Bedingungen für Überprüfungen

System- und Anwendungsereignisse, die im Zusammenhang mit der WDR RfA-CA stehen, werden anhand der Log-Dateien bei Verdachtsmomenten überprüft. Zusätzlich werden jährlich durch ein internes Audit die aufgezeichneten System- und Anwendungsereignisse sowie die Prozesse der WDR RfA-CA stichprobenhaft überprüft.

Es gelten die gleichen Regelungen in den WDR Sub-CAs und sind im kombiniertem CP/CPS Dokument zu dokumentieren.

8.2 Identität/Qualifikation des Prüfers

Der Prüfer verfügt über eine geeignete Qualifikation als Auditor . Es gelten die gleichen Regelungen in den WDR Sub-CAs und sind im kombiniertem CP/CPS Dokument zu dokumentieren.

8.3 Stellung des Prüfers zum Bewertungsgegenstand

Der Prüfer gehört weder zu der überprüften Abteilung noch ist er dieser Abteilung unterstellt. Es gelten die gleichen Regelungen in den WDR Sub-CAs und sind im kombiniertem CP/CPS Dokument zu dokumentieren.

8.4 Durch Überprüfungen abgedeckte Themen

Folgende Bereiche werden im Rahmen der Konformitätsprüfung mindestens untersucht:

- Prozesse des Zertifikatsmanagements

- Physikalische Sicherheitsmaßnahmen
- Technische Sicherheitsmaßnahmen
- Organisatorische Sicherheitsmaßnahmen
- Personelle Sicherheitsmaßnahmen

8.5 Reaktionen auf Unzulänglichkeiten

Wurden im Rahmen der Prüfung Mängel festgestellt, bewertet der IT-Sicherheitsbeauftragte des WDR die Prüfungsergebnisse mit den WDR RfA-CA Administratoren gemeinsam und entscheidet über das weitere Vorgehen. Die festgestellten Mängel werden priorisiert und geeignete Korrekturmaßnahmen prioritätengesteuert eingeleitet und koordiniert Es gelten die gleichen Regelungen in den WDR Sub-CAs und sind im kombiniertem CP/CPS Dokument zu dokumentieren.

8.6 Information über Bewertungsergebnisse

Die Ergebnisse des Audits werden dem Betreiber der Rundfunk-Root-CA und der CA-Steuerungsgruppe im Rahmen eines jährlichen Berichts zur Verfügung gestellt. Es gelten die gleichen Regelungen in den WDR Sub-CAs und sind im kombiniertem CP/CPS Dokument zu dokumentieren.

9 Andere geschäftliche und rechtliche Angelegenheiten

9.1 Gebühren

Für die Nutzung der WDR RfA-CA werden keine Gebühren erhoben.

9.2 Finanzielle Verantwortung

Finanzielle Aspekte werden in diesem Dokument nicht beschrieben.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Definition von vertraulichen Informationen

Jegliche Informationen über Teilnehmer und Antragsteller, die nicht unter den nächsten Abschnitt fallen, müssen als vertrauliche Informationen eingestuft und behandelt werden. Es gelten die gleichen Regelungen in den WDR Sub-CAs und sind im kombiniertem CP/CPS Dokument zu dokumentieren.

.

9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören

Alle Informationen, die in den veröffentlichten Zertifikaten und Sperrlisten enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft. Hierzu zählt z. B. der Name und Betreiber der RfA-CA.

9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen

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

verpflichtet wurden. Es gelten die gleichen Regelungen in den WDR Sub-CAs und sind im kombiniertem CP/CPS Dokument zu dokumentieren.

9.4 Schutz personenbezogener Daten

9.4.1 Datenschutzkonzept

Zur Leistungserbringung werden von der WDR RfA-CA personenbezogene Daten elektronisch gespeichert und verarbeitet. Dies geschieht in Übereinstimmung mit den entsprechenden Gesetzen. . Es gelten die gleichen Regelungen in den WDR Sub-CAs und sind im kombiniertem CP/CPS Dokument zu dokumentieren.

9.4.2 Als persönlich behandelte Daten

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.1 analog.

9.4.3 Daten, die nicht als persönlich behandelt werden

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.2 analog.

9.4.4 Zuständigkeiten für den Datenschutz

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.3 analog.

9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten

Der Zertifikatsnehmer stimmt der Nutzung von personenbezogenen Daten durch die WDR RfA-CA und WDR Sub-CA zu, soweit dies zur Leistungserbringung erforderlich ist. Darüber hinaus können alle Informationen veröffentlicht werden, 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 WDR RfA-CA unterliegt dem Recht des jeweiligen Staates und gibt vertrauliche und personenbezogene Informationen an staatliche Organe beim Vorliegen entsprechender Entscheidungen in Übereinstimmung mit den geltenden Gesetzen frei.

9.4.7 Andere Bedingungen für Auskünfte

Es sind keine weiteren Umstände für eine Veröffentlichung vorgesehen.

9.5 Urheberrechte

Keine weiteren Festlegungen.

9.6 Zusicherungen und Garantien der CA

Die WDR RfA-CA verpflichtet sich, die Anforderungen dieser Policy und der Rundfunk-Root-CA geeignet umzusetzen und ihre Aufgaben nach bestem Wissen und Gewissen durchzuführen.

9.6.1 Zusicherungen und Garantien der RA

Keine weiteren Festlegungen. Es gibt keine RA.

9.6.2 Zusicherungen und Garantien der Zertifikatsnehmer

Es gelten die Bestimmungen aus Abschnitt 4.5.1.

9.6.3 Zusicherungen und Garantien der Zertifikatsnutzer

Es gelten die Bestimmungen aus den Abschnitten 4.5.2, 4.9.6 und 6.1.7.

9.6.4 Zusicherungen und Garantien anderer Zertifikatsinfrastruktur-Teilnehmer

Keine weiteren Festlegungen. Es bestehen keine Zusicherungen und Garantien anderer Zertifikatsinfrastruktur-Teilnehmer.

9.7 Gewährleistung

Keine weiteren Festlegungen.

9.8 Haftungsbeschränkung

Keine weiteren Festlegungen.

9.9 Haftungsfreistellung

Keine weiteren Festlegungen.

9.10 Inkrafttreten und Aufhebung

9.10.1 Gültigkeitsdauer

Diese Policy tritt nach Veröffentlichung in Kraft. Sie wird einmal jährlich vom IT-Sicherheitsbeauftragten des WDR überprüft und die Ergebnisse werden dem ARD-Sternpunkt und der CA-Steuerungsgruppe im Rahmen ihres jährlichen Berichts vorgelegt.

9.10.2 Beendigung

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

9.10.3 Auswirkung der Beendigung und Weiterbestehen

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

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

Für Mitteilungen und Kommunikation unter den Teilnehmern der WDR PKI werden die internen Kommunikationsmittel des WDR verwendet.

9.12 Änderungen der Richtlinie

Die Erweiterung oder Modifikation dieses Dokuments liegt in der Verantwortung des Betreibers der WDR RfA-CA als Inhaber dieser Zertifizierungsrichtlinie.

9.13 Konfliktbeilegung

Keine weiteren Festlegungen.

9.14 Geltendes Recht

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

9.15 Konformität mit geltendem Recht

Die WDR 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 Weitere Regelungen

9.16.1 Vollständigkeitserklärung

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

9.16.2 Abgrenzungen

Keine weiteren Festlegungen.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Policy 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.

9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

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

9.16.5 Höhere Gewalt

Keine weiteren Festlegungen.

9.17 Andere Regelungen

Keine weiteren Festlegungen.