Certificate Policy (CP)/Certificate Policy Statement (CPS)

der Rundfunk-Root-CA

Version 2.0

Inhaltsverzeichnis

1. Einleitung

1.1 Überblick

Dieses Dokument ist eine Kombination der Certificate Policy (CP) und der Certificate Policy Statement (CPS) der Rundfunk-Root-CA.

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

1.2 Name und Kennzeichnung des Dokuments

Name: Certificate Policy (CP)/ Certificate Policy Statement (CPS) der Rundfunk-Root-CA

Version: 2.0

Datum: 19.06.2015

OID: 1.3.6.1.4.1.42638.1.1.2

1.3 Zertifikatsinfrastruktur-Teilnehmer

Teilnehmer können alle an das ARD-Daten-CN angeschlossenen Einrichtungen (Rundfunkanstalten, Gemeinschaftseinrichtungen und Dritte) sein. Die Rundfunk-Root-CA zertifiziert eine Sub-CA pro Teilnehmer des ARD-Daten-CN (im Folgenden RfA-CA genannt), sofern diese die Mindestanforderungen der Rundfunk-Root-CA an RfA-CAs erfüllt und die CA-Steuerungsgruppe der Aufnahme zugestimmt hat. Werden Teilnehmer vom ARD-Daten-CN ausgeschlossen oder beenden den Anschluss, endet automatisch auch die Mitgliedschaft an der Rundfunk-Root-CA.

Teilnehmer, die keine Verpflichtungen gegenüber der Rundfunk-Root-CA eingegangen sind, sind nicht Bestandteil dieser Richtlinie.

1.3.1 Zertifizierungsstellen

Der Rundfunk-Root-CA obliegt die Ausstellung von RfA-CA-Zertifikaten. Dabei kann jeder Teilnehmer des ARD-Daten-CN max. eine RfA-CA bei der Rundfunk-Root-CA zertifizieren lassen.

1.3.2 Registrierungsstellen

Nicht vorhanden.

1.3.3 Zertifikatsnehmer

Zertifikatsnehmer der Rundfunk-Root-CA sind RfA-CAs der Rundfunkanstalten.

1.3.4 Zertifikatsnutzer

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

1.3.5 Andere Teilnehmer

CA-Steuerungsgruppe

Festlegungen, die in diesem Dokument fehlen, werden von der CA-Steuerungsgruppe diskutiert und entschieden. Die CA-Steuerungsgruppe besteht aus je einem Vertreter der Teilnehmer, die sich von der Rundfunk-Root-CA haben zertifizieren lassen. Die genaue Beschreibung der Aufgaben ist in Kapitel 10.1 zu finden.

CA-Ansprechpartner

Jeder Teilnehmer der Rundfunk-Root-CA benennt einen CA-Ansprechpartner und einen Vertreter. Die CA-Ansprechpartner stehen dem Betreiber als technische Ansprechpartner zur Verfügung und beraten im Vorfeld für Themen, die von der CA-Steuerungsgruppe entschieden werden. Der Betreiber kontaktiert die CA-Ansprechpartner bei Bedarf.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

Die Rundfunk-Root-CA darf nur RfA-CA-Zertifikate ausstellen und muss die erlaubte Verwendung mittels der Zertifikatserweiterung KeyUsage bzw. ExtendedKeyUsage kennzeichnen.

1.4.2 Verbotene Verwendungen von Zertifikaten

Die Rundfunk-Root-CA darf keine Endnutzerzertifikate ausstellen und ihren privaten Schlüssel nicht zur Signatur, Entschlüsselung oder Authentisierung in Anwendungsprogrammen einsetzen.

1.5 Pflege der Richtlinie

1.5.1 Zuständigkeit für das Dokument

Verantwortlich für diese Richtlinie ist der IT-Sicherheitsbeauftragte des Betreibers der Rundfunk-Root-CA.

1.5.2 Ansprechpartner/Kontaktperson/Sekretariat

Ansprechpartner für diese CP/CPS ist der IT-Sicherheitsbeauftragte des Betreibers der Rundfunk-Root-CA.

Kontaktdaten siehe Anhang 10.2.

1.5.3 Pflege dieser Richtlinie

Diese Richtlinie wird vom IT-Sicherheitsbeauftragten des Betreibers einmal im Jahr auf Aktualität überprüft. Änderungswünsche können beim IT-Sicherheitsbeauftragten eingereicht und müssen von der CA-Steuerungsgruppe freigegeben werden.

1.5.4 Annahmeverfahren für Teilnehmer-CP

Eine RfA-CA, die sich von der Rundfunk-Root-CA zertifizieren lassen will, beantragt ihre Zertifizierung durch die Rundfunk-Root-CA beim Betreiber der Rundfunk-Root-CA. Die Beantragung umfasst eine Selbsterklärung (siehe Kapitel 10.3). Im Einzelnen erklärt er:

- dass seine RfA-CA den Anforderungen diesen Mindestanforderungen entspricht und
- dass in seinem CPS bzw. kombiniertem CP/CPS die Umsetzung dieser Anforderungen beschrieben ist.

Der Betreiber der Rundfunk-Root-CA überprüft die Konformität des CP/CPS dieses neuen Teilnehmers mit den Mindestanforderungen an eine RfA-CA. Entspricht das CP/CPS diesen Anforderungen, so legt der Betreiber den Antrag zur Genehmigung der CA-Steuerungsgruppe vor. Liegt die Genehmigung der CA-Steuerungsgruppe vor, stellt der Betreiber das entsprechende Zertifikat aus.

Entspricht das CP/CPS des neuen Teilnehmers den Anforderungen nicht in allen Punkten, wird der Antrag abgelehnt und der Antragsteller erhält die Möglichkeit zur Nachbesserung.

Der Teilnehmer stimmt zu, Änderungen im Zertifizierungsbetrieb, die nicht mit seiner bestehenden CP/CPS im Einklang stehen, wie auch die Beendigung seiner Zertifizierungsdienstleistungen, vorher der Rundfunk-Root-CA anzuzeigen.

Die Rundfunk-Root-CA ist nach Genehmigung der CA-Steuerungsgruppe berechtigt, wenn Teilnehmer diese Mindestanforderungen nicht erfüllen, die Zertifizierung durch die Rundfunk-Root-CA zu verweigern bzw. zu widerrufen.

Der Betreiber der Rundfunk-Root-CA kann eine erneute Abgabe der Selbsterklärung verlangen, wenn der Teilnehmer wesentliche Änderungen an seiner Zertifikatsinfrastruktur und/oder CP bzw. CPS vornimmt. Gleiches gilt, wenn diese Mindestanforderungen der Rundfunk-Root-CA wesentlich geändert wurden.

1.5.5 Zuständiger für die Anerkennung einer CP in Hinblick auf diese CP/CPS

Siehe 1.5.4

1.6 Begriffe und Abkürzungen

CA **Certification Authority**
Zertifizierungsstelle

CP **Certificate Policy**
Zertifizierungsrichtlinie

CPS **Certification Practice Statement**
Regelungen für den Zertifizierungsbetrieb

CSR **CertificateSigningRequest**
Zertifikatsantrag

DN **Distinguished Name**
Vollqualifizierter Name

DNS **Domain Name System**
Namensauflösung im Internet

HTTPS **Hypertext Transfer Protocol Secure**
Sicheres Hypertext-Übertragungsprotokoll

OCSP **Online Certificate Status Protocol**
Online-Auskunftsdienst zum Status von Zertifikaten

OID **Object Identifier**
Eindeutiger Kennzeichner für Objekte

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

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Die Rundfunk-Root-CA stellt all ihren Zertifikatsnutzern die unter 2.2 genannten Informationen auf einem Webserver unter https://www.cn.ard.de/kommunikationsnetze/zertifikate.htm bzw. http://certificate.cn.ard.de und http://certificate.ardstern.net zur Verfügung.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

Die Rundfunk-Root-CA veröffentlicht in den unter 2.1 genannten Verzeichnissen folgende aktuelle Informationen:

- Dieses kombinierte CP/CPS-Dokument
- Zertifikat der Rundfunk-Root-CA
- CRL der Rundfunk-Root-CA
- Kontaktinformationen, unter denen eine Sperrung beantragt werden kann
- Alle ausgestellten RfA-CA-Zertifikate

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

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

2.4 Zugriffskontrollen auf Verzeichnisse

Der Betreiber des Web-Servers, auf dem das Rundfunk-Root-CA-Zertifikat und Sperrinformationen der Rundfunk-Root-CA veröffentlicht werden, gewährleistet eine ordnungsgemäße Zugriffskontrolle, die unkontrollierte Änderungen dieser Informationen verhindert. Das Zertifikat und die Sperrliste der Rundfunk-Root-CA sind zum Schutz vor Manipulation durch eine digitale Signatur der Rundfunk-Root-CA gesichert. Somit kann jederzeit geprüft werden, ob die Integrität des Zertifikats und der Sperrliste noch gewährleistet ist. Allerdings existieren ggf. mehrere gültige Sperrlisten, sobald ein RfA-CA Zertifikat gesperrt wurde. Daher muss der Betreiber des Web-Servers durch eine geeignete Zugriffskontrolle sicherstellen, dass die aktuelle Sperrliste auf dem Web-Server nicht durch eine ältere – ebenfalls gültige – Sperrliste ersetzt wird.

3. Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

Die Namensgebung in Zertifikaten entspricht dem X.500 Standard.

3.1.2 Notwendigkeit für aussagefähige Namen

Für alle neuen RfA-CAs muss aus dem Namen im Zertifikat der Name der Rundfunkanstalt hervorgehen. Dabei wird im *subject* des Zertifikats in der CN-Komponente die Abkürzung der Rundfunkanstalt mit dem Zusatz „CA" (z.B. BR-CA, SWR-CA …), im O-Attribut der volle Name der Rundfunkanstalt und im C-Attribut „DE" stehen.

3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern

Es werden keine Pseudonyme verwendet, sondern die Zertifikate werden eindeutig den Rundfunkanstalten als Zertifikatsinhabern zugeordnet.

3.1.4 Regeln für die 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 die Rundfunkanstalt als den Zertifikatsinhaber enthalten, wie bspw. eine E-Mail Adresse.

3.1.5 Eindeutigkeit von Namen

Bei der Vergabe von Namen wird sichergestellt, dass der gewählte Distinguished Name (DN) innerhalb der Rundfunk-Root-CA eindeutig ist.

3.1.6 Anerkennung, Authentifizierung und Rolle von Markennamen

Keine weiteren Festlegungen.

3.2 Erstmalige Überprüfung der Identität

3.2.1 Methoden zur Überprüfung des Besitzes des privaten Schlüssels

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

3.2.2 Authentifizierung von Organisationszugehörigkeiten

Keine weiteren Festlegungen.

3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikatsnehmers

Der Zertifikatsantrag einer RfA-CA muss auf vertrauenswürdigem Wege an die Rundfunk-Root-CA Administratoren übermittelt werden. Zulässig ist die Beantragung via E-Mail mit Rückruf des Betreibers der Rundfunk-Root-CA an die vorab angegebene Telefonnummer des

CA-Ansprechpartners oder seines Vertreters oder die persönliche Übergabe eines Transfer-Datenträgers für den Zertifikatsantrag. Im Fall der persönlichen Übergabe erfolgt eine Ausweisprüfung, wenn der Antragsteller nicht persönlich bekannt ist.

3.2.4 Ungeprüfte Zertifikatsnehmerangaben

Keine weiteren Festlegungen.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Die Rundfunk-Root-CA stellt Zertifikate nur nach Prüfung der Berechtigung des Antragstellers aus. Berechtigter Antragsteller ist der CA-Ansprechpartner oder sein Vertreter, welche beide bei der Antragstellung zur Teilnahme dem Betreiber der Rundfunk-Root-CA schriftlich mit Angabe von Namen, Abteilung, Telefonnummer und E-Mail-Adresse benannt werden müssen.

3.2.6 Kriterien zur Zusammenarbeit

Für eine Zertifikatsinfrastruktur-übergreifende Zusammenarbeit müssen andere Zertifikatsinfrastrukturen die gleichen von der Rundfunk-Root-CA spezifizierten Mindestanforderungen erfüllen, die auch für die RfA-CAs gelten.

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

Im Unterschied zu einem Neuantrag zur Zertifizierung mit gesonderter Identitätsprüfung, erfolgt bei einer Zertifikatserneuerung keine gesonderte Identitätsprüfung, wenn die Authentifizierung auf Basis des noch gültigen Zertifikats der RfA-CA erfolgt. Ist das Zertifikat jedoch schon abgelaufen, gelten bei der Zertifikatserneuerung die gleichen Identifizierungs- und Authentifizierungsanforderungen wie beim Neuantrag (siehe Kapitel 3.2.3).

3.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen

Wurde das Zertifikat gesperrt, gelten bei der Zertifikatserneuerung die gleichen Identifizierungs- und Authentifizierungsanforderungen wie beim Neuantrag (siehe Kapitel 3.2.3).

3.4 Identifizierung und Authentifizierung von Sperranträgen

Sperranträge dürfen von jedermann gestellt werden und müssen von der CA-Steuerungsgruppe einstimmig freigegeben werden.

4. Betriebsanforderungen

4.1 Zertifikatsantrag

4.1.1 Wer kann einen Zertifikatsantrag stellen?

Zertifikatsanträge an die Rundfunk-Root-CA dürfen nur vom CA-Ansprechpartner einer RfA oder seinem Vertreter gestellt werden. Diese werden bei der Antragstellung zur Teilnahme an der Rundfunk-Root-CA in der Selbsterklärung benannt.

4.1.2 Registrierungsprozess und Zuständigkeiten

Der Antragsteller muss lokal ein Schlüsselpaar erzeugen und anschließend den öffentlichen Schlüssel gesichert in einem Zertifikatsantrag (CSR) bei der Rundfunk-Root-CA einreichen.

Zertifikate können nicht automatisiert bei der Rundfunk-Root-CA beantragt werden.

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Bei einer Zertifikatsbeantragung ist keine gesonderte Identitätsprüfung erforderlich, wenn der Antragsteller beim Betreiber bekannt ist.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Keine weiteren Festlegungen.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Zertifikatsanträge werden innerhalb von fünf Werktagen bearbeitet.

4.3 Zertifikatsausgabe

4.3.1 Aktionen des Zertifizierungsdiensteanbieters bei der Ausgabe von Zertifikaten

Eine Ausgabe von Zertifikaten erfolgt nur für gültige Zertifikatsanträge, die syntaktisch korrekt sind und alle erforderlichen Informationen im Antrag enthalten.

Der Zertifikatsantrag einer RfA-CA muss auf vertrauenswürdigem Wege an die CA-Administratoren der Rundfunk-Root-CA übermittelt werden. Zulässig ist die Beantragung via E-Mail mit Rückruf an die vorab angegebene Telefonnummer des CA-Ansprechpartners oder seines Vertreters oder die persönliche Übergabe eines Transfer-Datenträgers für den Zertifikatsantrag. Im Fall der persönlichen Übergabe muss eine Ausweisprüfung erfolgen, wenn der Antragsteller nicht persönlich bekannt ist (siehe auch 3.2.3).

USB-Speichersticks mit Zertifikatsanträgen von anderen Teilnehmern des ARD-Daten-CN werden zunächst auf einem „Schleusenrechner" beim ARD-Sternpunkt gescannt, bevor sie an der virtuellen Maschine der Rundfunk-Root-CA angeschlossen werden. Auf dem Schleusenrechner sind zwei Virenscanner von anderen Herstellern als der Virenscanner auf dem Arbeitsplatzlaptop installiert.

Die Ausstellung eines RfA-CA Zertifikats ist nur im Vier-Augen-Prinzip zulässig, d. h. durch einen der CA-Administratoren vom ARD-Sternpunkt und dem Sachgebietsleiter CN vom ARD-

Sternpunkt oder Sebastian Beyermann. Nach Ausstellung des RfA-CA Zertifikats fertigt der CA-Administrator eine schriftliche Protokollnotiz über den Vorgang an und archiviert diese in einem Ordner im Safe im A-Bau. Außerdem verteilt er die Information über das neu ausgestellte RfA-CA Zertifikat an die CA-Ansprechpartner.

Nach der Ausstellung eines RfA-CA-Zertifikats wird ein manuelles Backup der Rundfunk-Root-CA Datenbank und der Log-Dateien erstellt. Der CA-Administrator brennt die Backup-Daten auf ein optisches Speichermedium, das im Safe des ARD-Sternpunkts im T-Bau aufbewahrt wird.

4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats durch die Rundfunk-Root-CA

Es erfolgt keine explizite Benachrichtigung vom Betreiber der Rundfunk-Root-CA an den CA-Ansprechpartner der RfA-CA und seinen Vertreter. Die Benachrichtigung ist der Erhalt des RfA-CA-Zertifikats, das ihnen entweder per E-Mail oder auf einem Datenträger übermittelt wird. Die Art der Zertifikatsübergabe richtet sich nach der Art, wie der Zertifikatsantrag eingereicht wurde.

4.4 Zertifikatsannahme

4.4.1 Verhalten für eine Zertifikatsannahme

Keine weiteren Festlegungen.

4.4.2 Veröffentlichung des Zertifikats durch die Rundfunk-Root-CA

Alle ausgestellten RfA-CA-Zertifikate werden auf
https://www.cn.ard.de/kommunikationsnetze/zertifikate.htm veröffentlicht.

4.4.3 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe des Zertifikats

Der Betreiber der Rundfunk-Root-CA informiert nach Ausstellung eines neuen RfA-CA-Zertifikats die CA-Ansprechpartner über die Ausstellung des neuen RfA-CA-Zertifikats.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Die Rundfunk-Root-CA darf ihren Schlüssel und Zertifikat nur für die im Zertifikat genannten Verwendungszwecke einsetzen, d.h. zur Ausstellung von untergeordneten CA-Zertifikaten und Sperrlisten. Sie darf ihre privaten Schlüssel nicht zur Signatur, Entschlüsselung oder Authentisierung in Anwendungsprogrammen einsetzen.

Eine RfA-CA darf ihren Schlüssel und Zertifikat nur für die im Zertifikat genannten Verwendungszwecke einsetzen, d.h. zur Ausstellung von CA-Zertifikaten, Endnutzerzertifikaten und Sperrlisten. Sie darf ihre privaten Schlüssel nicht zur Signatur, Entschlüsselung oder Authentisierung in Anwendungsprogrammen einsetzen.

Die Rundfunk-Root-CA und alle RfA-CAs müssen Sorge tragen, dass ihr privater Schlüssel angemessen geschützt ist. Das Zertifikat einer RfA-CA darf nur in Übereinstimmung mit den Mindestanforderungen der Rundfunk-Root-CA eingesetzt werden. Das Zertifikat ist unverzüg-

lich zu sperren, wenn die Angaben des Zertifikats nicht mehr korrekt sind oder wenn der private Schlüssel abhandengekommen, gestohlen oder möglicherweise kompromittiert wurde.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

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

4.6 Zertifikatserneuerung

Im Fall einer Zertifikaterneuerung für die Rundfunk-Root-CA oder eine RfA-CA findet zwingend auch eine Schlüsselerneuerung statt (siehe Kapitel 4.7).

4.7 Zertifizierung nach Schlüsselerneuerung

Bei einer Zertifikaterneuerung mit Schlüsselwechsel wird einem Zertifikatsnehmer, der bereits ein Zertifikat besitzt, durch die Rundfunk-Root-CA ein neues Zertifikat für ein neues Schlüsselpaar ausgestellt, sofern die im Zertifikat enthaltenen Informationen unverändert bleiben.

4.7.1 Bedingungen für eine Zertifizierung nach Schlüsselerneuerung

Eine Zertifikaterneuerung mit Schlüsselwechsel kann beantragt werden, wenn z.B. die Gültigkeit eines Zertifikats abläuft. Sie muss zwingend beantragt werden, wenn ein Zertifikat aufgrund von Schlüsselkompromittierung gesperrt wurde.

4.7.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen?

Eine Schlüssel- und Zertifikatserneuerung wird grundsätzlich durch den CA-Ansprechpartner der RfA-CA oder seinen Vertreter beantragt.

4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Siehe Kapitel 4.3.1. Dabei ist der Rückruf bei der Beantragung via E-Mail nicht nötig.

4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Es erfolgt keine explizite Benachrichtigung vom Betreiber der Rundfunk-Root-CA an den CA-Ansprechpartner der RfA-CA und seinen Vertreter. Die Benachrichtigung ist der Erhalt des Nachfolgezertifikats, das ihnen entweder per E-Mail oder auf einem Datenträger übermittelt wird. Die Art der Zertifikatsübergabe richtet sich nach der Art, wie der Zertifikatsantrag eingereicht wurde.

4.7.5 Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen

Keine weiteren Festlegungen.

4.7.6 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die Rundfunk-Root-CA

Es gelten die Regelungen gemäß Abschnitt 4.4.2.

4.7.7 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Der Betreiber informiert nach der Schlüsselerneuerung eines RfA-CA-Zertifikats die CA-Ansprechpartner und die CA-Steuerungsgruppe über die Ausgabe des Nachfolgezertifikats.

4.8 Zertifikatsänderung

4.8.1 Bedingungen für eine Zertifikatsänderung

Haben sich Angaben in einem Zertifikat geändert, so muss eine Zertifikatsänderung beantragt und durchgeführt werden.

Technisch bedeutet dies die Sperrung des alten Zertifikats und eine Zertifikatserneuerung (siehe Abschnitt 4.6).

4.8.2 Wer darf eine Zertifikatsänderung beantragen?

Eine Zertifikatsänderung darf grundsätzlich nur durch den CA-Ansprechpartner der RfA-CA oder seinem Vertreter beantragt werden.

4.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung

Siehe Kapitel 4.3.1.

4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Es erfolgt keine explizite Benachrichtigung vom Betreiber der Rundfunk-Root-CA an den CA-Ansprechpartner der RfA-CA und seinen Vertreter. Die Benachrichtigung ist der Erhalt des neuen RfA-CA-Zertifikats, das ihnen entweder per E-Mail oder auf einem Datenträger übermittelt wird. Die Art der Zertifikatsübergabe richtet sich nach der Art, wie der Zertifikatsantrag eingereicht wurde.

4.8.5 Verhalten für die Annahme einer Zertifikatsänderung

Keine weiteren Festlegungen.

4.8.6 Veröffentlichung der Zertifikatsänderung durch die Rundfunk-Root-CA

Es gelten die Regelungen gemäß Abschnitt 4.4.2.

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

Der Betreiber informiert nach Zertifikatsänderung eines RfA-CA-Zertifikats die CA-Ansprechpartner und die CA-Steuerungsgruppe über die Ausgabe des neuen RfA-CA-Zertifikats.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Bedingungen für eine Sperrung

Ein RfA-CA Zertifikat muss gesperrt werden, wenn mindestens einer der folgenden Gründe vorliegt:

- Das Zertifikat enthält Angaben, die nicht mehr gültig sind.

- Der private Schlüssel der RfA-CA wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
- Die RfA-CA ist nicht mehr berechtigt, das Zertifikat zu nutzen.
- Die RfA-CA hält die von der Rundfunk-Root-CA vorgegebenen Mindestanforderungen nicht ein.
- Die RfA-CA stellt den Zertifizierungsbetrieb ein.

4.9.2 Wer kann eine Sperrung beantragen?

Sperranträge können von jedermann gestellt werden. Die CA-Steuerungsgruppe prüft diese Anträge und entscheidet dann darüber, ob dem Antrag stattgegeben wird. Die Freigabe eines Sperrantrags erfordert die Einstimmigkeit der CA-Steuerungsgruppe.

4.9.3 Verfahren für einen Sperrantrag

Besteht der Verdacht, dass ein Grund für eine Sperrung (siehe Kapitel 4.9.1) eingetreten ist, wird ein Sperrantrag bei der Rundfunk-Root-CA gestellt. Wird die Sperrung nicht vom jeweiligen CA-Ansprechpartner oder seinem Vertreter beantragt, muss sie durch die CA-Steuerungsgruppe einstimmig freigegeben werden.

Die Durchführung der Sperrung von RfA-CA Zertifikaten erfolgt nur im Vier-Augen-Prinzip, d. h. durch einen der CA-Administratoren vom ARD-Sternpunkt und dem Sachgebietsleiter CN vom ARD-Sternpunkt oder Sebastian Beyermann. Nach der Sperrung eines RfA-CA Zertifikats und der Ausstellung einer neuen Sperrliste fertigt der CA-Administrator eine schriftliche Protokollnotiz über den Vorgang an und archiviert diese in einem Ordner im Safe im A-Bau. Außerdem verteilt er die Information über das gesperrte RfA-CA Zertifikat an alle CA-Ansprechpartner. Abschließend wird die neue Sperrliste exportiert und unter http://certificate.cn.ard.de und http://certificate.ardstern.net publiziert.

Nach der Sperrung eines RfA-CA-Zertifikats muss ein manuelles Backup der Rundfunk-Root-CA Datenbank und der Log-Dateien erfolgen. Der CA-Administrator brennt die Backup-Daten auf ein optisches Speichermedium, das im Tresor des ARD-Sternpunkts im T-Bau aufbewahrt wird.

4.9.4 Fristen für einen Sperrantrag

Bei Bekanntwerden eines Sperrgrundes muss unverzüglich die Sperrung beantragt werden.

4.9.5 Fristen/Zeitspanne für die Bearbeitung des Sperrantrags durch die Rundfunk-Root-CA

Eine Zertifikatssperrung muss unverzüglich erfolgen.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Die Rundfunk-Root-CA stellt den Zertifikatsprüfern Sperrinformationen zu ihren ausgestellten RfA-CA Zertifikaten in Form von Sperrlisten zur Verfügung. Diese werden auf einem Webserver unter http://certificate.cn.ard.de und http://certificate.ardstern.net veröffentlicht.

4.9.7 Frequenz der Veröffentlichung von Sperrlisten

Die Sperrliste der Rundfunk-Root-CA ist maximal 13 Monate gültig. Es wird mindestens jährlich (alle 12 Monate) eine neue Sperrliste erstellt. Im Falle einer Sperrung eines Zertifikats muss zusätzlich eine neue Sperrliste ausgestellt und veröffentlicht werden, die ebenfalls wie-

der maximal 13 Monate gültig ist. Diese wird spätestens 24 Stunden nach durchgeführter Sperrung des entsprechenden RfA-CA Zertifikates veröffentlicht.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die Latenzzeit für Sperrlisten (Zeitpuffer zwischen dem regulärem Ausstellungszeitpunkt und der tatsächlichen Veröffentlichung der Sperrliste) beträgt maximal einen Monat, d. h. die Sperrliste ist einen Monat länger gültig als der Ausstellungszyklus der Sperrliste.

4.9.9 Verfügbarkeit von Online-Sperrinformationen

Die Rundfunk-Root-CA bietet keinen Online-Dienst zur Auskunft der Gültigkeit von Zertifikaten an.

4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen

Entfällt.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Es gibt keine weiteren Formen zur Anzeige von Sperrinformationen.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Bei Bekanntwerden der Kompromittierung des privaten Schlüssels der Rundfunk-Root-CA oder eines hinreichenden Verdachts darauf muss das Zertifikat der Rundfunk-Root-CA unverzüglich gesperrt werden.

4.9.13 Bedingungen für eine Suspendierung

Eine temporäre Sperrung bzw. eine Suspendierung von Zertifikaten findet nicht statt und ist auch für RfA-CAs nicht erlaubt.

4.9.14 Wer kann eine Suspendierung beantragen?

Entfällt.

4.9.15 Verfahren für Anträge auf Suspendierung

Entfällt.

4.9.16 Begrenzungen für die Dauer von Suspendierungen

Entfällt.

4.10 Statusabfragedienst für Zertifikate

Die Rundfunk-Root-CA bietet keinen Statusabfragedienst für die ausgestellten RfA-CA Zertifikate an.

4.11 Kündigung durch den Zertifikatsnehmer

Im Fall einer Kündigung durch eine RfA-CA wird ihr Zertifikat gesperrt.

4.12 Schlüsselhinterlegung und Wiederherstellung

Die Rundfunk-Root-CA bietet keine Schlüsselhinterlegung und Wiederherstellung von Schlüsseln für RfA-CAs an.

5. Nicht-technische Sicherheitsmaßnahmen

Die Gewährleistung geeigneter infrastruktureller, organisatorischer und personeller Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb der Rundfunk-Root-CA.

5.1 Bauliche Sicherheitsmaßnahmen

5.1.1 Lage und Gebäude

Da die Rundfunk-Root-CA eine Offline-CA ist und als virtuelle Maschine auf einer Festplatte betrieben wird, wird diese in einem Safe im A-Bau auf dem Gelände des HR aufgehoben. Die Smartcard, auf der sich der private Schlüssel befindet, wird auch im gleichen Safe gelagert.

5.1.2 Zugang

Den Schlüssel zum Safe haben nur der Sachgebietsleiter vom ARD-Hörfunkstern und sein Vertreter.

5.1.3 Strom, Heizung und Klimaanlage

Keine weiteren Festlegungen.

5.1.4 Wassergefährdung

Gefährdungen durch Wasser sind hinreichend ausgeschlossen.

5.1.5 Brandschutz

Es ist ein geeigneter Brandschutz vorhanden.

5.1.6 Lager und Archiv

Das Backup der Rundfunk-Root-CA wird in einem anderen Safe als die Produktivumgebung in einem Safe im T-Bau auf dem Gelände des HR gelagert. Zugriff zu diesem Safe haben der Leiter des ARD-Sternpunkts und die IT-Sicherheitsbeauftragte.

5.1.7 Datenvernichtung

Bei der Entsorgung von Papierdokumenten und elektronischen Datenträgern wird sichergestellt, dass alle sicherheitsrelevanten, vertraulichen oder personenbezogenen Daten vernichtet werden.

5.1.8 Disaster-Recovery-Backup

Zu Disaster-Recovery-Zwecken wird das jeweils neueste Backup der Rundfunk-Root-CA in einem Safe im T-Bau auf dem Gelände des HR aufbewahrt. Fünf Sicherheitskopien des Rundfunk-Root-CA Schlüssels und die zugehörigen Passwortbriefe werden in jeweils einem Safe beim WDR, BR, NDR, SWR und ZDF aufbewahrt. Dabei besitzt keine Rundfunkanstalt den passenden Passwortbrief zur Smartcard. Eine genaue Verteilung der Smartcards und PIN-Briefe findet sich im Anhang 10.5.

5.2 Verfahrensvorschriften

5.2.1 Rollenkonzept

Folgende Rollen sind besetzt:

Rolle	Typ der Rolle	Mindestanzahl der Personen	Aufgabe
Lokaler Administrator der Rundfunk-Root-CA VM	Betriebssystem	2	Verwaltet die Rundfunk-Root-CA VM.
Rundfunk-Root-CA Administrator	Zertifikatsinfrastruktur	2	Konfiguriert und wartet die Rundfunk-Root-CA. Erneuert bei Bedarf das CA-Zertifikat. Ist auch verantwortlich für die Zertifikatsausstellung und ggf. -sperrung für RfA-CAs. Übernimmt die Veröffentlichung der Rundfunk-Root-CA Sperrliste.
Tresorverwalter für Tresor des ARD-Sternpunkts im A-Bau	Schließregelung	1	Verwahrt die externe Festplatte mit der Rundfunk-Root-CA VM und die produktive Smartcard der Rundfunk-Root-CA.
Tresorverwalter für Tresor des ARD-Sternpunkts im T-Bau	Schließregelung	1	Verwahrt: • Backup der virtuellen Maschine der Rundfunk-Root-CA auf einem optischen Speichermedium • Backup der Rundfunk-Root-CA Datenbank und Log-Dateien auf einem optischen Speichermedium • Passwort des lokalen System Administrators der Rundfunk-Root-CA VM • PIN/PUK-Brief der produktiven CA-Smartcard
Tresorverwalter andere RfA	Schließregelung	je 1 bei WDR, BR, NDR, SWR	Verwahrt eine Ersatz-Smartcard der Rund-

Rolle	Typ der Rolle	Mindestanzahl der Personen	Aufgabe
		und ZDF	funk-Root-CA und einen nicht dazu passenden PIN/PUK-Brief.
CA-Steuerungsgruppe	Zertifikatsinfrastruktur	Je 1 von jedem Mitglied	Entscheidet gemeinsam über die: • Aufnahme von neuen Mitgliedern • Sperrung von RfA-CAs • Pflege der Mindest-anforderungen Entwicklung von Zertifi-katsvorgaben
CA-Ansprechpartner	Zertifikatsinfrastruktur	Je 1 von jedem Mitglied	Stehen dem Betreiber als technische An-sprechpartner zur Ver-fügung und beraten im Vorfeld über Themen, die von der CA-Steuerungsgruppe ent-schieden werden.

5.2.2 Mehraugenprinzip

Alle Aufgaben – außer den Tresorverwaltern - werden nur im Mehraugenprinzip durchgeführt. Für die beiden Rollen „Lokaler Administrator der Rundfunk-Root-CA VM" und „Rundfunk-Root-CA Administrator" sind jeweils zwei Personen vorgesehen, um ein Vier-Augen-Prinzip umzusetzen. „Zwei Augen" für die beiden Rollen sind die Augen des Sachgebietsleiters CN vom ARD-Sternpunkt oder seines Vertreters, die anderen „zwei Augen" stammen von einem der beiden Rundfunk-Root-CA Administratoren beim ARD-Sternpunkt.

5.2.3 Identifizierung und Authentifizierung jeder Rolle

Zur Authentifizierung bei allen Rollen genügt eine Ein-Faktor-Authentifizierung: Benutzername und Passwort.

5.2.4 Rollentrennung

Die beiden Rollen „Lokaler System Administrator der Rundfunk-Root-CA VM", und „Rundfunk-Root-CA Administrator" sind zwar konzeptionell getrennt, werden aber von den gleichen Personen übernommen, d. h. die Personen, die als „Lokaler Administrator der Rundfunk-Root-CA VM" auftreten, agieren auch als „Rundfunk-Root-CA Administrator".

Die Rolle eines Tresorverwalter wird nicht in Personalunion mit der Rolle „Lokaler Administrator der Rundfunk-Root-CA VM" und „Rundfunk-Root-CA Administrator" übernommen, so dass

die Zugriffsberechtigung für die Rundfunk-Root-CA von der physischen Zugriffsberechtigung auf die externe Festplatte mit der Rundfunk-Root-CA VM getrennt ist und somit keine Rolle alleine Zugriff und Zugang zu der Rundfunk-Root-CA hat. Zugriff auf den Tresor beim ARD-Sternpunkt im A-Bau, in dem die externe Festplatte aufbewahrt wird, hat der Sachgebietsleiter Hörfunk vom ARD-Sternpunkt oder sein Vertreter. Zugriff auf den Tresor beim ARD-Sternpunkt im T-Bau haben der Leiter des ARD-Sternpunkts und die IT-Sicherheitsbeauftragte.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

Die Rundfunk-Root-CA Administratoren kennen den Stand der Technik und die Best Practises im Bereich Zertifikatsinfrastruktur.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Eine Sicherheitsüberprüfung der Rundfunk-Root-CA Administratoren findet nicht statt.

5.3.3 Anforderungen an Schulungen

Es gibt keine Anforderungen an Schulungen.

5.3.4 Häufigkeit von Schulungen und Belehrungen

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

5.3.5 Häufigkeit und Folge von Job-Rotation

Es finden keine Job-Rotationen statt.

5.3.6 Maßnahmen bei unerlaubten Handlungen

Die Sanktionen werden den üblichen arbeitsrechtlichen Maßnahmen angepasst.

5.3.7 Anforderungen an freie Mitarbeiter

Externe Mitarbeiter und unabhängige, selbstständige Zulieferer haben nur in Begleitung von berechtigten ARD-Sternpunkt-Mitarbeitern Zutritt und Zugriff auf die Rundfunk-Root-CA.

5.3.8 Dokumente, die dem Personal zur Verfügung gestellt werden müssen

Den Rundfunk-Root-CA Administratoren wird vor Beginn des Betriebes dieses Dokument zur Verfügung gestellt.

5.4 Überwachungsmaßnahmen

5.4.1 Arten von aufgezeichneten Ereignissen

Alle sicherheitsrelevanten Ereignisse der Rundfunk-Root-CA werden in Log-Dateien protokolliert.

5.4.2 Häufigkeit der Bearbeitung der Aufzeichnungen

Nur bei Verdachtsmomenten wird eine Prüfung der Log-Protokolle (Aufzeichnungen) durchgeführt.

5.4.3 Aufbewahrungszeit von Aufzeichnungen

Das jeweils aktuelle Backup des Log-Protokolls (Aufzeichnungen) der Rundfunk-Root-CA wird mindestens während der gesamten Laufzeit der Rundfunk-Root-CA aufbewahrt.

5.4.4 Sicherung der Aufzeichnungen

Die Protokolldaten (Aufzeichnungen) werden auf ein optisches Speichermedium gebrannt, das im Tresor des ARD-Sternpunkts im T-Bau aufbewahrt wird. So sind sie gegen unberechtigten Zugriff, Löschung und Manipulation geschützt.

5.4.5 Datensicherung der Aufzeichnungen

Nach jeder signifikanten Änderung an der Rundfunk-Root-CA oder ihrer Konfiguration – besonders nach der Ausstellung oder Sperrung eines RfA-CA-Zertifikats – erfolgt ein manuelles Backup der Rundfunk-Root-CA Datenbank und der Log-Dateien, das der CA-Administrator auf ein optisches Speichermedium brennt.

5.4.6 Speicherung der Aufzeichnungen (intern / extern)

Das optische Speichermedium mit den Protokolldaten (Aufzeichnungen) wird im Tresor des ARD-Sternpunkts im T-Bau auf dem Gelände des HR aufbewahrt.

5.4.7 Benachrichtigung der Ereignisauslöser

Es findet keine automatische Benachrichtigung bei schwerwiegenden Ereignissen wie Konfigurationsänderungen der Rundfunk-Root-CA oder dem Import von Zertifikaten und privaten Schlüsseln statt.

5.4.8 Schwachstellenanalyse

Der Arbeitsplatzrechner, auf dem die virtuelle Maschine ausgeführt wird, ist in das Patch-Management des ARD-Sternpunkts integriert und verfügt über aktuelle Software und einen Virenscanner.

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen

Fünf Sicherheitskopien des Rundfunk-Root-CA Schlüssels und die zugehörigen Passwortbriefe werden in jeweils einem Safe beim WDR, BR, NDR, SWR und ZDF aufbewahrt. Dabei besitzt keine Rundfunkanstalt den passenden Passwortbrief zur Smartcard. Eine genaue Verteilung der Smartcards und PIN-Briefe findet sich im Anhang 10.5.

Des Weiteren werden Zertifikats-, Sperranträge und Log-Dateien archiviert und im Safe im T-Bau auf dem Gelände des HR aufbewahrt.

5.5.2 Aufbewahrungsfristen für archivierte Daten

Die Sicherungskopien des Rundfunk-Root-CA-Schlüssels, das Zertifikat sowie das hinterlegte Passwort werden während der gesamten Verwendungsdauer des privaten Rundfunk-Root-CA-Schlüssels aufbewahrt. Gleiches gilt für die Zertifikats-, Sperranträge und aktuellen Log-Dateien.

5.5.3 Sicherung des Archivs

Die Sicherungskopien des Rundfunk-Root-CA-Schlüssels sowie die Passwörter für die Sicherungskopie werden vor unberechtigtem Zugriff geschützt in verschiedenen Safes aufbewahrt.

5.5.4 Datensicherung des Archivs

Es wird keine Datensicherung des Archivs vorgenommen.

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

Keine weiteren Festlegungen.

5.5.6 Archivierung (intern / extern)

Keine weiteren Festlegungen.

5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen

Keine weiteren Festlegungen.

5.6 Schlüsselwechsel der Rundfunk-Root-CA

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

Beim Schlüsselwechsel der Rundfunk-Root-CA wird neues Schlüsselmaterial generiert, das alte Schlüsselmaterial wird nicht beibehalten.

5.7 Kompromittierung und Geschäftsweiterführung bei der Rundfunk-Root-CA

5.7.1 Behandlung von Vorfällen und Kompromittierungen

Bei Verlust der Smartcard mit dem Rundfunk-Root-CA Schlüssel oder versehentlicher Löschung der Smartcard wird eine der Ersatzkarten mit der Sicherungskopie des Rundfunk-Root-CA-Schlüssels verwendet.

Falls im Laufe der Gültigkeitsdauer des Rundfunk-Root-CA Zertifikats die verwendeten Kryptoverfahren bzw. Schlüssellängen (siehe Kapitel 6.1 und 7.1) nicht mehr als hinreichend sicher zu betrachten sind, wird die CA-Steuerungsgruppe informiert, welches über die nächsten Schritte entscheidet.

5.7.2 Rechnerressourcen-, Software- und/oder Datenkompromittierung

Im Verdachtsfall von kompromittierter Software oder Daten werden die Daten aus einer unkompromittierten Datensicherung zurückgespielt. Kompromittierte Software oder Daten bedeuten dabei, dass Software oder Daten manipuliert sein könnten oder der Eigentümer des Systems keine Kontrolle mehr über die korrekte Funktionsweise oder den korrekten Inhalt hat.

5.7.3 Verhalten bei Kompromittierung des privaten Schlüssels der Rundfunk-Root-CA

Bei hinreichendem Verdacht auf eine Kompromittierung des privaten Schlüssels der Rundfunk-Root-CA wird unverzüglich die Sperrung des Rundfunk-Root-CA Zertifikats bekannt gegeben sowie alle ausgestellten RfA-CA Zertifikate gesperrt. Zum Aufbau einer neuen Zertifikatsinfrastruktur werden neue Schlüssel für die Rundfunk-Root-CA erzeugt, ein neues Rundfunk-Root-CA Zertifikat ausgestellt und alle RfA-CAs neu zertifiziert. Die RfA-CAs können dabei ihre Schlüssel beibehalten.

5.7.4 Möglichkeiten zur Geschäftsweiterführung nach einer Kompromittierung

Die Wiederaufnahme des Betriebs nach einer Kompromittierung wird in den vorangegangen Kapiteln 5.7.1, 5.7.2. und 5.7.3 beschrieben.

5.8 Schließung der Rundfunk-Root-CA

Wenn die Rundfunk-Root-CA ihren Betrieb einstellt, und von ihr ausgestellte Zertifikate noch gültig sind, werden diese gesperrt. Anschließend wird von der Rundfunk-Root-CA eine letzte Sperrliste ausgestellt, die bis zum Ende der Laufzeit ihres CA-Zertifikats gültig ist. Außerdem werden alle Smartcards mit dem privaten Schlüssel der Rundfunk-Root-CA sicher vernichtet.

Bei Einstellung des Betriebs der Rundfunk-Root-CA wird das Datum der Außerbetriebnahme in diesem Dokument eingetragen. Außerdem wird ein Bericht über die ordnungsgemäße Außerbetriebnahme erstellt, in dem u.a. die Nichtwiederherstellbarkeit der Schlüssel der Rundfunk-Root-CA bestätigt wird.

6. Technische Sicherheitsmaßnahmen

Die Gewährleistung geeigneter technischer Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb einer Zertifikatsinfrastruktur.

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

Das Schüsselpaar der Rundfunk-Root-CA wird in Software erzeugt und auf sechs Smartcards (eine Produktiv- und fünf Backup-Smartcards) gespeichert.

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Die Rundfunk-Root-CA erstellt keine privaten Schlüssel für RfA-CAs.

6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

Der CSR des Antragstellers, der den öffentlichen Schlüssel der RfA-CA enthält, wird per E-Mail, HTTPS oder auf einem Datenträger an die Rundfunk-Root-CA übermittelt.

6.1.4 Lieferung öffentlicher CA-Schlüssel an Zertifikatsprüfer (Relying Parties)

Der öffentliche Schlüssel der Rundfunk-Root-CA muss als Vertrauensanker sicher an die RfA-CA übermittelt werden. Der öffentliche Schlüssel einer RfA-CA wird von der Rundfunk-Root-CA zertifiziert. Dieses RfA-CA-Zertifikat wird den Zertifikatsprüfern von der RfA-CA selbst zur Verfügung gestellt.

6.1.5 Schlüssellängen

Die Rundfunk-Root-CA verwendet das RSA-Verfahren und eine Schlüssellänge von 4096 Bit. Die Schlüsselpaare von RfA-CAs müssen eine Schlüssellänge von mindestens 2048 Bit aufweisen. Bei Migration einer bereits bestehenden Zertifikatsinfrastruktur unter die Rundfunk-Root-CA dürfen kürzere Schlüssellängen für Endnutzer oder -systeme noch bis zum Ablauf des Zertifikats genutzt werden. Die Verwendung von Schlüssellängen unter 1024 Bit ist nicht zulässig.

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 entsprechenden Anforderungen aus FIPS 140-2.

6.1.7 Schlüsselverwendungen

Die Rundfunk-Root-CA verwendet ihren privaten Schlüssel nur zur Ausstellung von RfA-CA-Zertifikaten und Sperrlisten. Auch RfA-CAs dürfen ihren privaten Schlüssel nur zur Ausstellung von Zertifikaten und Sperrlisten einsetzen.

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

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

Der private CA-Schlüssel der Rundfunk-Root-CA wurde in sechs Smartcards (JCOP 21 bzw. SmartCafeExpert 4.0) importiert. Eine Smartcard wird produktiv genutzt, fünf Smartcards dienen als Backup. Der private Schlüssel wird nur in den Smartcards verwendet und ist nicht mehr auslesbar. Smartcards sind nach ISO 7816 standardisiert.

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

Der Zugriff auf den privaten Schlüssel der Rundfunk-Root-CA ist nur im Vier-Augen-Prinzip möglich. Den einen Teil der PIN der produktiven Smartcard kennen die beiden Rundfunk-Root-CA Administratoren und den zweiten Teil der Sachgebietsleiter CN bzw. Sebastian Beyermann. Die PINs für die Ersatz-Smartcards sind in zwei getrennten Umschlägen aufbewahrt.

6.2.3 Hinterlegung privater Schlüssel

Die Rundfunk-Root-CA bietet keine Hinterlegung privater Schlüssel an.

6.2.4 Sicherung privater Schlüssel

Fünf Sicherheitskopien des Rundfunk-Root-CA Schlüssels und die zugehörigen Passwortbriefe werden in jeweils einem Safe beim WDR, BR, NDR, SWR und ZDF aufbewahrt. Dabei besitzt keine Rundfunkanstalt den passenden Passwortbrief zur Smartcard. Eine genaue Verteilung der Smartcards und PIN-Briefe findet sich im Anhang 10.5 (siehe Abschnitt 5.5).

6.2.5 Archivierung privater Schlüssel

Die Sicherungskopie des privaten RfA-CA-Schlüssels sowie die PIN für die Sicherungskopie werden durch Aufbewahrung in verschiedenen Safes vor unberechtigtem Zugriff geschützt (siehe Abschnitt 5.5).

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Die Schlüsselerzeugung der Rundfunk-Root-CA erfolgte in Software. Der private Schlüssel wurde danach direkt in die Smartcards importiert (siehe Abschnitt 6.2.1) und anschließend auf der Festplatte sicher gelöscht.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Der private Schlüssel der Rundfunk-Root-CA ist auf Smartcards gespeichert (JCOP 21 bzw. SmartCafeExpert 4.0) und ist somit nicht mehr auslesbar.

6.2.8 Aktivierung privater Schlüssel

Der private Schlüssel der Rundfunk-Root-CA kann nur nach Eingabe der PIN aktiviert werden. Anschließend ist er für den weiteren Gebrauch frei geschaltet.

6.2.9 Deaktivierung privater Schlüssel

Der private Schlüssel der Rundfunk-Root-CA wird deaktiviert durch Ziehen der Smartcard aus dem Kartenleser oder durch Beendigung der Zertifikatsdienste.

6.2.10 Zerstörung privater Schlüssel

Um den privaten Schlüssel der Rundfunk-Root-CA zu löschen, wird die produktive Smartcard physisch zerstört. Die Vernichtung des privaten Schlüssels umfasst auch die Smartcards mit den Sicherungskopien des privaten Schlüssels, die in jeweils einem Safe beim WDR, BR, NDR, SWR und ZDF aufbewahrt werden.

6.2.11 Beurteilung kryptographischer Module

Keine weiteren Festlegungen.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Es werden keine öffentlichen Schlüssel archiviert.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Das Rundfunk-Root-CA-Zertifikat ist 30 Jahre gültig. Der private Schlüssel wird jedoch nur solange zur Ausstellung neuer untergeordneter Zertifikate verwendet, wie das Gültigkeitsende der ausgestellten Zertifikate noch im Gültigkeitsbereich der Rundfunk-Root-CA liegt.

6.4 Aktivierungsdaten

6.4.1 Aktivierungsdaten

Die PIN zur Aktivierung des privaten Schlüssels der Rundfunk-Root-CA ist vier Zeichen lang.

6.4.2 Schutz von Aktivierungsdaten

Zwei Zeichen sind dem Rundfunk-Root-CA Administrator, die anderen beiden Zeichen sind dem Sachgebietsleiter CN und Sebastian Beyermann bekannt. Für den Notfall ist die PIN aufgeteilt in zwei Briefumschläge im Safe des ARD-Sternpunkts im T-Bau hinterlegt.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Die Rundfunk-Root-CA läuft in einer VM, welche auf einer externen Festplatte gespeichert ist. Aufbewahrt wird die Festplatte im Safe des ARD-Sternpunkts im A-Bau. Sowohl der lokale System Administrator als auch der Rundfunk-CA-Administrator haben ein Passwort bestehend aus 12 Zeichen. Beide Passwörter sind in zwei Teile geteilt: Sechs Zeichen sind dem Rundfunk-Root-CA Administrator bzw. dem lokalen System Administrator, die anderen sechs Zeichen sind dem Sachgebietsleiter CN und Sebastian Beyermann bekannt. Weitere Benutzer haben keinen Zugriff auf die VM.

6.5.2 Beurteilung von Computersicherheit

Keine weiteren Festlegungen.

6.6 Technische Maßnahmen während des Life Cycles

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

Es findet keine Entwicklung statt.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Aktuelle Updates und Patches für das Betriebssystem, auf dem die VM ausgeführt wird, werden eingespielt, bevor Arbeiten an dieser vorgenommen werden.

6.6.3 Sicherheitsmaßnahmen während der Life Cycles

Keine weiteren Festlegungen.

6.7 Sicherheitsmaßnahmen für Netze

Die VM wird auf einem Arbeitsplatzrechner betrieben, der während des Betriebs der Rundfunk-Root-CA nicht im Netzwerk des ARD-Sternpunkts hängt.

6.8 Zeitstempel

Keine weiteren Festlegungen.

7. Profile von Zertifikaten, Sperrlisten und OCSP

7.1 Zertifikatsprofile

7.1.1 Versionsnummern

Die Versionsnummer im Zertifikat wird auf den Wert 2 gesetzt. Dieser Wert kennzeichnet X.509 Zertifikate mit Erweiterungen.

7.1.2 Zertifikatserweiterungen

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

- BasicConstraints (Basiseinschränkungen)
- KeyUsage (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 werden außerdem weitere nicht-kritische Zertifikatserweiterungen in den RfA-CA-Zertifikaten ergänzt.

7.1.3 Algorithmen OIDs

Es wird der Algorithmus „sha256WithRSAEncryption" verwendet.

7.1.4 Namensformate

Siehe Kapitel 3.1.4

7.1.5 Namensbeschränkungen

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

7.1.6 OIDs der Zertifikatsrichtlinien

In allen von der Rundfunk-Root-CA ausgestellten RfA-CA-Zertifikaten wird dieses CP/CPS-Dokument über den in Kapitel 1.2 angegebenen OID referenziert, d.h. dieser OID wird als Policy-Identifier in der CertificatePolicies Erweiterung in allen ausgestellten Zertifikaten eingetragen.

7.1.7 Nutzung der Erweiterung "Policy Constraints"

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

7.1.8 Syntax und Semantik von "Policy Qualifiers"

Keine weiteren Festlegungen.

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung Zertifikatsrichtlinie

Keine weiteren Festlegungen.

7.2 Sperrlistenprofile

7.2.1 Versionsnummer(n)

Die Versionsnummer der Sperrliste wird auf den Wert 1 gesetzt. Dieser Wert kennzeichnet X.509 Sperrlisten mit Erweiterungen.

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

In den Sperrlisten der 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 werden weitere nicht kritische Erweiterungen in den Sperrlisten ergänzt.

7.3 Profile des Statusabfragedienstes (OCSP)

7.3.1 Versionsnummer(n)

Es wird kein OCSP angeboten.

7.3.2 OCSP Erweiterungen

Es wird kein OCSP angeboten.

8. Überprüfungen und andere Bewertungen

8.1 Häufigkeit und Bedingungen für Überprüfungen

System- und Anwendungsereignisse, die im Zusammenhang mit der Zertifizierungsinfrastruktur 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 Rundfunk-Root-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

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 Betreibers der Rundfunk-Root-CA die Prüfungsergebnisse mit dem Rundfunk-Root-CA Administrator gemeinsam und entscheidet über das weitere Vorgehen. Die festgestellten Mängel werden priorisiert und geeignete Korrekturmaßnahmen prioritätengesteuert eingeleitet und koordiniert.

8.6 Information über Bewertungsergebnisse

Die Ergebnisse des Audits werden der CA-Steuerungsgruppe im Rahmen des jährlichen Berichts zur Verfügung gestellt.

9. Andere finanzielle und rechtliche Angelegenheiten

9.1 Preise

Es werden keine Gebühren für die Nutzung der Rundfunk-Root-CA erhoben.

9.2 Finanzielle Zuständigkeiten

9.2.1 Versicherungsdeckung

Keine weiteren Festlegungen.

9.2.2 Andere Posten

Keine weiteren Festlegungen.

9.2.3 Versicherung oder Gewährleistung für Endnutzer

Keine weiteren Festlegungen.

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

9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen

Jede von der Rundfunk-Root-CA zertifizierte RfA-CA trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen. Vertrauliche 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.

9.4 Datenschutz von Personendaten

9.4.1 Datenschutzkonzept

Die Rundfunk-Root-CA speichert elektronisch und verarbeitet zur Leistungserbringung personenbezogene Daten, z. B. Namen und Kontaktdaten der CA-Ansprechpartner der teilnehmenden RfA. Dies erfolgt in Übereinstimmung mit den entsprechenden Gesetzen.

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 Reglungen aus Abschnitt 9.3.2 analog.

9.4.4 Zuständigkeiten für den Datenschutz

Für personenbezogene Daten gelten die Reglungen 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 Rundfunk-Root-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

Alle von der Rundfunk-Root-CA zertifizierten RfA-CAs unterliegen dem Recht des jeweiligen Landes und müssen vertrauliche und personenbezogene Informationen an staatliche Organe beim Vorliegen entsprechender Entscheidungen in Übereinstimmung mit den geltenden Gesetzen freigeben.

9.4.7 Andere Bedingungen für Auskünfte

Es sind keine weiteren Umstände für eine Veröffentlichung vorgesehen.

9.5 Geistiges Eigentumsrecht

Der Betreiber der Rundfunk-Root-CA ist Urheber des vorliegenden Dokuments. Eine Weitergabe von veränderten Fassungen dieser Richtlinie ist ohne Zustimmung des Betreibers nicht zulässig.

9.6 Zusicherungen und Garantien

9.6.1 Zusicherungen und Garantien der Rundfunk-Root-CA

Der Betreiber der Rundfunk-Root-CA verpflichtet sich, die Inhalte dieser CP/CPS geeignet umzusetzen und seine Aufgaben nach bestem Wissen und Gewissen durchzuführen.

9.6.2 Zusicherungen und Garantien der RA

Es gibt keine RA.

9.6.3 Zusicherungen und Garantien der Zertifikatsnehmer

Es gelten die Bestimmungen aus Abschnitt 4.5.1.

9.6.4 Zusicherungen und Garantien der Zertifikatsnutzer

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

9.6.5 Zusicherungen und Garantien anderer Zertifikatsinfrastruktur-Teilnehmer

Keine weiteren Festlegungen.

9.7 Haftungsausschlüsse

Keine weiteren Festlegungen.

9.8 Haftungsbeschränkungen

Keine weiteren Festlegungen.

9.9 Schadensersatz

Keine weiteren Festlegungen.

9.10 Gültigkeitsdauer und Beendigung

9.10.1 Gültigkeitsdauer

Dieses CP/CPS-Dokument tritt nach Veröffentlichung in Kraft. Die Aktualität des Dokuments wird jährlich einmal vom IT-Sicherheitsbeauftragten des Betreibers der Rundfunk-Root-CA überprüft und die Ergebnisse der CA-Steuerungsgruppe im jährlichen Bericht vorgelegt.

9.10.2 Beendigung

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

9.10.3 Auswirkung der Beendigung und Weiterbestehen

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

9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern

Keine weiteren Festlegungen.

9.12 Ergänzungen

9.12.1 Verfahren für Ergänzungen

Eine Änderung dieses CP/CPS-Dokuments kann nur durch den Betreiber der Rundfunk-Root-CA mit Genehmigung der CA-Steuerungsgruppe erfolgen.

9.12.2 Benachrichtigungsmechanismen und –fristen

Bei Änderungen dieses CP/CPS-Dokuments werden alle RfA-CAs innerhalb von einem Monat informiert.

9.12.3 Bedingungen für OID Änderungen

Werden Änderungen in diesem Dokument vorgenommen, die sicherheitsrelevante Aspekte betreffen, ist eine Änderung der OID dieses Dokuments erforderlich (siehe Abschnitt 1.2). Alle zukünftig von der Rundfunk-Root-CA ausgestellten Zertifikate enthalten dann die neue OID des geänderten CP/CPS-Dokuments.

9.13 Verfahren zur Schlichtung von Streitfällen

Keine weiteren Festlegungen.

9.14 Zugrunde liegendes Recht

Der Betrieb der Rundfunk-Root-CA unterliegt den Gesetzen der Bundesrepublik Deutschland.

9.15 Einhaltung geltenden Rechts

Die Rundfunk-Root-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 CP/CPS 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 CP/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.

9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

Rechtliche Auseinandersetzungen, die aus dem Betrieb der Rundfunk-Root-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 Bestimmungen

Keine weiteren Bestimmungen.

10. Anhang

10.1 Aufgaben der CA-Steuerungsgruppe und der CA-Ansprechpartner

CA-Steuerungsgruppe und CA-Ansprechpartner beschäftigten sich nur mit organisatorischen und infrastrukturellen und nicht mit anwendungsspezifischen Aufgaben.

Die CA-Steuerungsgruppe hat folgende Aufgaben:

- ***Aufnahme von neuen Mitgliedern:*** Grundsätzlich können alle Teilnehmer des ARD-Daten-CN einen Antrag stellen. Nachdem der Betreiber geprüft hat, dass CP und CPS den Mindestanforderungen entsprechen, entscheidet die CA-Steuerungsgruppe über die Aufnahme. Die Entscheidung muss einstimmig sein.

- ***Sperrung von RfA-CAs:*** Grundsätzlich können Sperranträge von jedermann gestellt werden. Die Sperranträge werden durch die CA-Steuerungsgruppe freigegeben. Dabei muss die Entscheidung einstimmig sein. Das betroffene Mitglied darf an der Abstimmung nicht teilnehmen.

- ***Pflege der Mindestanforderungen:*** Änderungen an den Mindestanforderungen werden vom Betreiber der Rundfunk-Root-CA vorgeschlagen. Diese müssen von der CA-Steuerungsgruppe freigegeben werden.

- ***Entwicklung von Zertifikatsvorgaben:*** Werden neue Dienste gemeinsam genutzt, werden vom Betreiber der Rundfunk-Root-CA die entsprechenden Mindestanforderungen und evtl. speziell benötigte Zertifikatsinhalte festgelegt. Diese müssen von der CA-Steuerungsgruppe freigegeben werden.

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. Der Betreiber der Rundfunk-Root-CA kontaktiert die CA-Ansprechpartner bei Bedarf.

Nach der Aufnahme, Ausstellung oder Sperrung eines RfA-CA-Zertifikats werden die CA-Ansprechpartner und Vertreter vom Betreiber informiert.

10.2 Kontaktdaten

IT-Sicherheitsbeauftragte des Betreibers der Rundfunk-Root-CA

Dominique Mähler

ARD-Sternpunkt

Bertramstraße 8

60320 Frankfurt

Tel +49/69/59677-404

Fax +49/69/59677-199

E-Mail: dominique.maehler@ard-stern.de

10.3 Jährliche Arbeiten des Betreibers

Der Betreiber führt im Rahmen der Neuausstellung der Sperrliste (CRL) folgende Arbeiten durch:

- Vollständige Sicherung der virtuellen Maschine auf einen optischen Datenträger
- Überprüfung der eingesetzten Hard- und Software auf Aktualität
- Überprüfung der eingesetzten Kryptoverfahren und Schlüssellängen auf Aktualität
- Überprüfung bei den RfAn, die eine Ersatz-Smartcard im Safe liegen haben:
    - Ob Ansprechpartner noch aktuell
    - Ob Siegel unbeschädigt
    - Die Siegelnummer noch die gleiche ist

Der Betreiber erstellt jährlich einen Gesamtbericht und stellt ihn der CA-Steuerungsgruppe zur Verfügung. Dieser Bericht enthält Folgendes:

- Ergebnisse der jährlichen Arbeiten
- Ergebnisse der internen Audits der Mitglieder

10.4 Antrag und Selbsterklärung zur Teilnahme an der Rundfunk - Zertifikatsinfrastruktur

Der ARD-Sternpunkt betreibt die Rundfunk – Zertifikatsinfrastruktur zur Bereitstellung von digitalen Zertifikaten und übernimmt dazu die Rolle der zentralen Certification Authority (CA). Alle Teilnehmer am Corporate Network der ARD (ARD-Daten-CN) haben grundsätzlich die Möglichkeit, diese Infrastruktur auf Antrag zu nutzen. Dies ist sowohl durch Anschluss einer eigenen Zertifikatsinfrastruktur als auch durch Nutzung der zentralen Zertifikatsinfrastruktur im Service möglich.

Innerhalb der Rundfunk – Zertifikatsinfrastruktur werden ausschließlich nicht öffentliche Zertifikate verwendet. Durch den Austausch von Zertifikaten mit Dritten kann zu diesen eine Vertrauensstellung etabliert werden, die alle angeschlossenen Teilnehmer nutzen können.

Die Nutzung der Rundfunk – Zertifikatsinfrastruktur (wie z.B. für einen übergreifenden WLAN-Zugang) obliegt ausschließlich den teilnehmenden Anstalten, die für diese Nutzung auch die Verantwortung tragen. Alle Teilnehmer erkennen den Betreiber der Rundfunk – Zertifikatsinfrastruktur als vertrauenswürdige Instanz an.

Alle Teilnehmer der Rundfunk – Zertifikatsinfrastruktur verpflichten sich dauerhaft zum ordnungsgemäßen Betrieb der teilnehmerinternen Zertifikatsinfrastruktur (RfA-CA) und der teilnehmerinternen Registration Authority (RA) unter Einhaltung der gemeinsam festgelegten

Mindestanforderungen. Sie benennen je einen technischen Ansprechpartner (CA-Ansprechpartner).

Zudem entsenden Sie einen Vertreter in die CA-Steuerungsgruppe, die über die Aufnahme und den Ausschluss von Teilnehmern entscheidet, den Betreiber kontrolliert sowie die Mindestanforderungen aktualisiert und für alle Teilnehmer inkl. einer Frist zur Umsetzung verbindlich festschreibt. Die CA-Steuerungsgruppe ist jederzeit berechtigt, einen Teilnehmer, der die Mindestverpflichtungen nicht (mehr) einhält, zu deregistrieren. Dieser Beschluss ist einstimmig unter Enthaltung des betroffenen Teilnehmers zu fällen.

Teilnahmevoraussetzungen

Jeder Teilnehmer an der Rundfunk – Zertifikatsinfrastruktur hat zusammen mit diesem Aufnahmeantrag folgende Unterlagen bereitzustellen und verpflichtet sich, diese fortan umzusetzen und aktuell zu halten:

- Certificate Policy (CP)
  Dieses Dokument beschreibt das Regelwerk der Teilnehmer-Zertifizierungsstelle und insbesondere die Methoden zur Einhaltung der Mindestanforderungen. Als Muster können hierfür die Mindestanforderungen an die Teilnehmer verwendet werden.

- Certification Practice Statement (CPS)
  Dieses Dokument beschreibt die konkrete Umsetzung des Regelwerks der CP beim Teilnehmer.

Die Aufnahme erfolgt nur dann, wenn der Betreiber nach Prüfung der vorgelegten Unterlagen die Einhaltung der Mindestanforderungen durch den Antragsteller bestätigt und die CA-Steuerungsgruppe den Antrag einstimmig annimmt.

Der Antragsteller erklärt sich zudem bereit, jederzeit notwendige Anpassungen an der teilnehmerinternen Zertifikatsinfrastruktur vorzunehmen, falls dies zur Aufrechterhaltung der Interoperabilität z.B. infolge der technischen Fortentwicklung erforderlich ist.

Der Antragsteller verpflichtet sich jede Änderung an der teilnehmerinternen Zertifikatsinfrastruktur bzw. der CP oder CPS dem Betreiber und der CA-Steuerungsgruppe unverzüglich anzuzeigen. Dies gilt insbesondere für den Fall der Betriebseinstellung der teilnehmerinternen Zertifikatsinfrastruktur.

Der Antrag ist nach dem Vier-Augen-Prinzip von zwei verantwortlichen MitarbeiterInnen des Antragstellers zu unterzeichnen. Als „Antragsteller 1" wird eine Person in der Verantwortung eines Hauptabteilungsleiters erwartet, die beim Antragsteller für die Informationstechnik verantwortlich ist. Die Benennung des „Antragstellers 2" obliegt dem Teilnehmer eigenverantwortlich.

Antrag

Bezeichnung des Teilnehmers

Anschrift

Antragsteller 1

Nachname, Vorname

Bereich, Abteilung

Telefonnummer

E-Mail-Adresse

Antragsteller 2

Nachname, Vorname

Bereich, Abteilung

Telefonnummer

E-Mail-Adresse

Mitglied in der CA-Steuerungsgruppe

Nachname, Vorname

Bereich, Abteilung

Telefonnummer

E-Mail-Adresse

CA-Ansprechpartner

Nachname, Vorname

Bereich, Abteilung

Telefonnummer

E-Mail-Adresse

Vertreter des CA-Ansprechpartners

Nachname, Vorname

Bereich, Abteilung

Telefonnummer

E-Mail-Adresse

Zu veröffentlichende URLs

CP-Dokument

Zertifikat der RfA-CA

Liste der zur RfA-CA gehörenden RAs

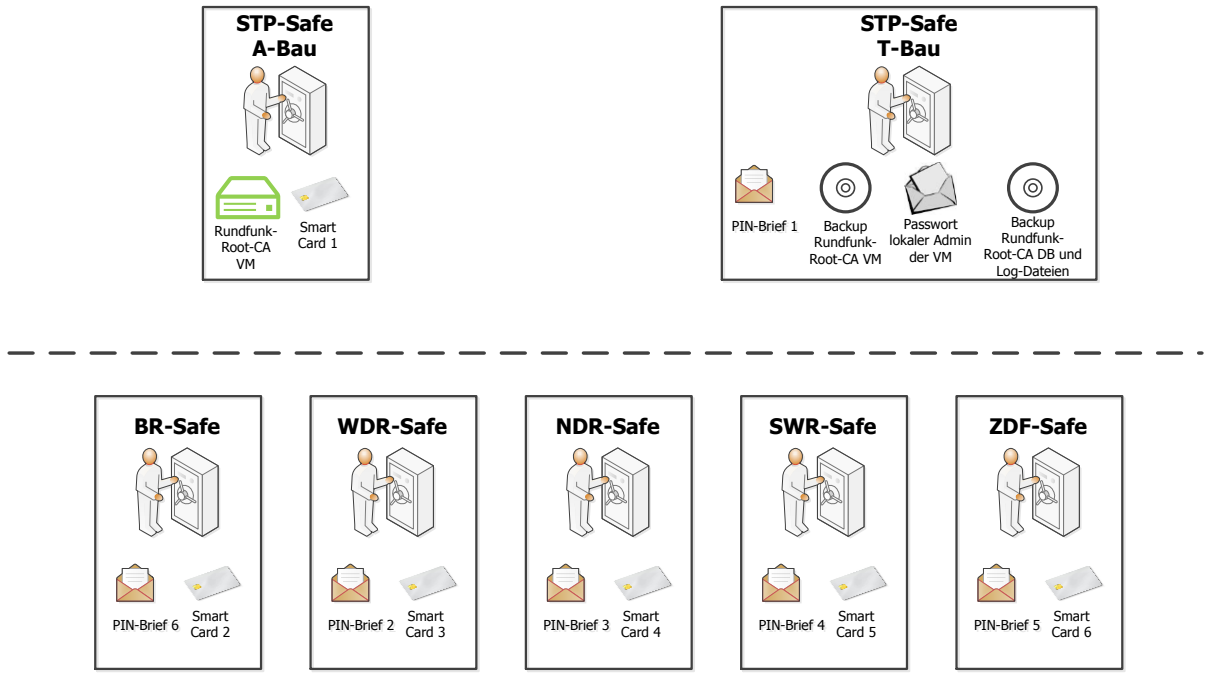
Zertifikatsverzeichnisdienst
(soweit betrieben)

Sperrliste (CRL) der RfA-CA

Sperrkontakt

10.5 Übersicht Safe

Safe-Übersicht für die Rundfunk-Root-CA



Stand: 24.10.2013