Westdeutscher Rundfunk
CP Offline WDR-CA

Zertifizierungsrichtlinie der WDR-CA für die WDR Sub-CAs

Pezhman Pedramfar Alexander Gast

27. Dezember 2023

Westdeutscher Rundfunk
Appellhofplatz 1
D-50667 Köln

www.wdr.de

Inhaltsverzeichnis

Disclaimer

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

1 Einleitung

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

Das vorliegende Dokument bezieht sich auf die Version 3.4 der Mindestanforderungen (CP) der Rundfunk-Root-CA und Version 2.0 des CPS-Dokumentes für die WDR-CA.

1.1 Überblick

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

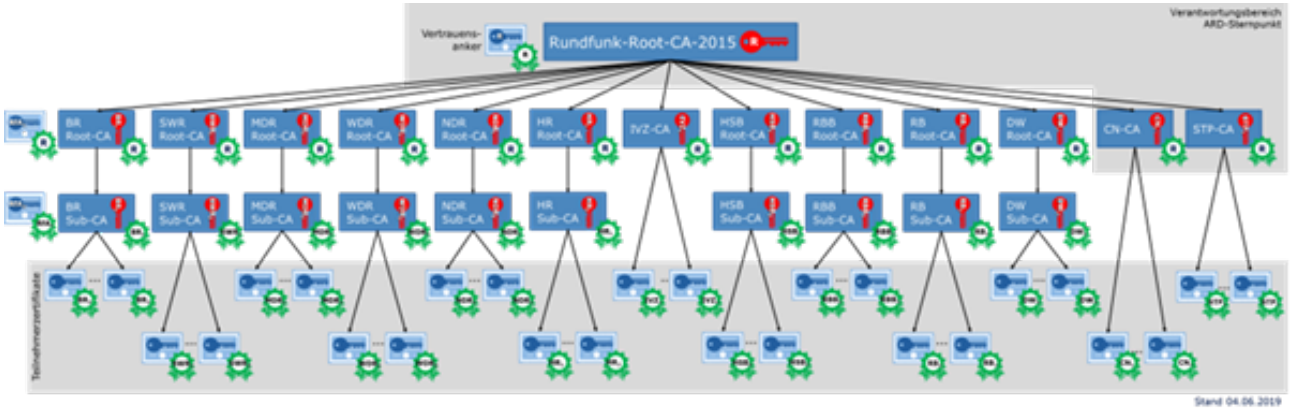

Abbildung 1.1: Beispielhafter Überblick über die Zertifikatsinfrastruktur des ARD-Netzes

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

In weiteren, separaten Dokumenten sind das Certificate Practice Statement (CPS) der **RfA**-CA, und die Certificate Practice Statements (CPS) für die **RfA** Sub-CAs niedergelegt. Die **RfA** Sub-CAs werden in virtuellen Maschinen (VMs) innerhalb eines Virtualisierungsclusters oder containerisiert (Docker,

OCI) innerhalb von Kubernetes-Umgebungen betrieben. Durch die Auslegung auf Cluster-Systemen ist ein Mindestmaß an Ausfallsicherheit umgesetzt. Das Schlüsselmaterial liegt unabhängig der Umsetzung auf den HSM-Modulen der **RfA**.

1.2 Name und Kennzeichnung des Dokuments

Name	Zertifizierungsrichtlinie (CP) der WDR-CA für die WDR-Sub-CAs
Version	2.0
Datum	27. Dezember 2023
OID	1.3.6.1.4.1.42638.1.7.1.2.0

1.3 Zertifikatsinfrastruktur-Teilnehmer

Teilnehmer können alle an das ARD-Netz angeschlossenen Einrichtungen (Rundfunkanstalten, Gemeinschaftseinrichtungen und Dritte) sein. Die Rundfunk-Root-CA zertifiziert eine Sub-CA pro Teilnehmer des ARD-Netzes (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. Für die Übergangszeit bei Zertifikatserneuerung oder bei der Migration zu einer neuen **RfA**-CA kann ein zweites RfA-Zertifikat für den gleichen Zweck ausgestellt werden. Die Übergangszeit beträgt maximal 24 Monate. Wird die Migration vor Ende der Übergangszeit abgeschlossen, ist der Teilnehmer verpflichtet das alte RfA-Zertifikat sperren zu lassen (siehe auch Abschnitt 4.9.1).

In Ausnahmefällen kann es nötig sein, dass für einen Teilnehmer mehr als eine **RfA**-CA ausgestellt oder die Übergangsfrist verlängert wird. Diese Ausnahme muss von der CA-Steuerungsgruppe genehmigt werden. Die Ausnahmen werden in diesem Dokument In Kapitel 10.2 aufgelistet. Werden Teilnehmer vom ARD- Netz ausgeschlossen oder beenden den Anschluss, wird das Zertifikat der jeweiligen RfA-CA gesperrt und es 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 Mindestanforderungen.

1.3.1 Zertifizierungsstellen

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

Die **RfA** Sub-CA darf nur Endanwenderzertifikate ausstellen.

1.3.2 Registrierungsstellen

Eine **RfA** Sub-CA benötigt eine Registrierungsstelle (RA) zur Überprüfung der Identität und Authentizität von Zertifikatsnehmern, sofern eine gesonderte Identitätsprüfung erforderlich ist (siehe Kapitel

3.2.3). Die **RfA**-RA kann auch für weitere **RfA** Sub-CAs zuständig sein.

1.3.3 Zertifikatsnehmer

Zertifikatsnehmer einer **RfA** Sub-CA dürfen natürliche Personen, Funktionsaccounts und technische Systeme (Maschinen, Server und Netzwerkkomponenten) innerhalb der **RfA** sein. Eine **RfA** Sub-CA darf keine weiteren CA-Zertifikate ausstellen. Eine weitergehende genauere Regelung kann in dem CPS Dokument der **RfA** Sub-CA definiert werden. Die Zuweisung von Zertifikaten an Funktionsaccounts muss auf definierte Anwendungsfälle beschränkt und im CPS Dokument der **RfA** Sub-CA dokumentiert werden.

1.3.4 Zertifikatsnutzer

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

1.3.5 Andere Teilnehmer

Der Betreiber einer **RfA** Sub-CA entsendet keinen Vertreter in die CA-Steuerungsgruppe. Sofern eine **RfA** Sub-CA nicht von den gleichen Personen betrieben wird wie die **RfA**-CA, muss dem Betreiber der **RfA**-CA bei der Registrierung ein technischer Ansprechpartner für die jeweilige **RfA** Sub-CA benannt werden.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

Eine **RfA** Sub-CA, die sich von der **RfA**-CA zertifizieren lassen will, darf nur Endanwenderzertifikate für Personen, Funktionsaccounts und technische Systeme (Maschinen, Server und Netzwerkkomponenten) ausstellen. Sie muss die erlaubte Verwendung des ausgestellten Zertifikats mittels der Zertifikatserweiterung `KeyUsage` und optional `ExtendedKeyUsage` kennzeichnen.

1.4.2 Verbotene Verwendungen von Zertifikaten

Eine **RfA** Sub-CA darf keine weiteren Sub-CA Zertifikate ausstellen. Eine **RfA** Sub-CA darf ihren Schlüssel nicht zu Verschlüsselungs- oder Authentisierungszwecken oder für andere Signaturen als zur Zertifikats- oder Sperrlistenausstellung nutzen.

1.5 Pflege der Mindestanforderungen

1.5.1 Zuständigkeit für das Dokument

Eine **RfA** Sub-CA muss eine Zuständige für ihre eigene Zertifizierungsrichtlinie (CP) und/oder Regelungen für den Zertifizierungsbetrieb (CPS) benennen. Zuständig für dieses Dokument sind Herr Pezhman Pedramfar und Herr Alexander Gast als Vertreter des Betreibers der **RfA** Sub-CA.

1.5.2 Ansprechpartner/Kontaktperson/Sekretariat

Eine **RfA** Sub-CA muss einen Ansprechpartner für ihre eigene Zertifizierungsrichtlinie (CP) und/oder Regelungen für den Zertifizierungsbetrieb (CPS) benennen, der bei Fragen hierzu von der **RfA**-CA oder anderen berechtigten Stellen kontaktiert werden kann.

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

1.5.3 Pflege dieser Mindestanforderungen

Eine **RfA** Sub-CA muss einmal im Jahr ihre eigene Zertifizierungsrichtlinie und/oder Regelungen für den Zertifizierungsbetrieb auf Aktualität und Erhalt der Konformität zur jeweils aktuellen Fassung dieser Anforderungen der **RfA**-CA überprüfen. Eine bloße Korrektur auf sprachlicher Ebene (Schreibfehler, Grammatikfehler u. ä.) ist keine Änderung in diesem Sinne und erfordert keine formale Freigabe.

1.5.4 Annahmeverfahren für Teilnehmer-CP

Eine **RfA** Sub-CA muss dem Betreiber der **RfA**-CA ihrerseits bei Zertifikatsbeantragung ein CPS Dokument vorlegen, in dem der Zertifizierungsbetrieb und die Umsetzung der Anforderungen dieser Zertifizierungsrichtlinie beschrieben sind, und erklären, dass sie die Anforderungen der **RfA**-CA einhält. Alle in diesem Policy-Dokument genannten Anforderungen an **RfA** Sub-CAs sind verbindlich und können nicht abgeschwächt werden. Vor Zertifikatsausstellung prüft die **RfA**-CA das Policy-Dokument der **RfA** Sub-CA. Erfüllt die **RfA** Sub-CA die in diesem Dokument beschriebenen Anforderungen der **RfA**-CA nicht, wird die Zertifizierung von der **RfA**-CA abgelehnt oder nachträglich widerrufen.

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

Siehe 1.5.4

1.6 Begriffe und Abkürzungen

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

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

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

2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Eine **RfA** Sub-CA, die sich von der **RfA**-CA zertifizieren lässt, muss all ihren Zertifikatsnutzern ihr eigenes CA-Zertifikat und Sperrinformationen zu den von ihr ausgestellten Zertifikaten auf dem PKI-Veröffentlichungspunkt (Repository) bereitstellen. Bei der Veröffentlichung von Zertifikaten muss sie sicherstellen, dass eine mögliche Veröffentlichung personenbezogener Daten nicht den geltenden Datenschutzrichtlinien widerspricht. Eine **RfA** Sub-CA muss Verzeichnisdienste nutzen, deren ordnungsgemäßer Betrieb sichergestellt ist, die sich an geltenden Sicherheitsrichtlinien der RfA und dem aktuellen Stand der Technik orientieren.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

Eine **RfA** Sub-CA, die sich von der **RfA**-CA zertifizieren lässt, muss all ihren Zertifikatsnutzern:

- das CP oder das kombinierte CP-/CPS-Dokument
- das Zertifikat der Sub-CA und dessen Fingerabdruck
- den Verweis auf einen Verzeichnisdienst für die ausgestellten Zertifikate, sofern ein solcher betrieben wird
- die CRL der Sub-CA
- die Kontaktinformationen, unter denen eine Sperrung beantragt werden kann

auf einem Webserver im **RfA**-internen LAN und optional im AD zur Verfügung stellen.

Werden die Endanwenderzertifikate einer **RfA** Sub-CA für ARD-Netz-weit angebotene Dienste verwendet, müssen diese nicht nur RfA intern, sondern auch RfA-übergreifend geprüft werden können. Hierfür müssen die oben genannten Informationen nicht nur im RfA-internen LAN, sondern auch auf einem Webserver im ARD-Netz veröffentlicht werden. Sofern eine **RfA** Sub-CA Zertifikate ausstellt, die außerhalb des RfA und außerhalb des ARD-Netzes genutzt werden, muss sie die oben genannten Informationen auch im Internet verfügbar machen und sicherstellen, dass auch die CA-Zertifikate und die Sperrinformationen der anderen CAs in der Zertifikatskette im Internet verfügbar sind.

Den Zertifikatsnehmern (Endanwendern) sollten Informationen über die korrekte Anwendung von Kryptographie und über die sichere Verwendung von Zertifikaten zur Verfügung gestellt werden.

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Die Veröffentlichung von Sperrinformationen muss unverzüglich spätestens 24 Stunden nach durchgeführter Sperrung des entsprechenden Zertifikates erfolgen.

2.4 Zugriffskontrollen auf Verzeichnisse

Unkontrollierte Änderungen von Zertifikaten und Sperrinformationen im AD sowie auf den Webservern für den Zugriff aus dem **RfA** internen LAN, im ARD-Netz und im Internet müssen verhindert werden. Der lesende Zugriff auf die Informationen muss ohne vorherige Anmeldung möglich sein. Der schreibende Zugriff ist auf berechtigte Personen zu beschränken. Zertifikate und Sperrlisten sind zum Schutz vor Manipulation durch eine digitale Signatur zu sichern. Somit kann jederzeit geprüft werden, ob die Integrität der Zertifikate und Sperrlisten gewährleistet ist und ob sie von einem vertrauenswürdigen Herausgeber stammt.

3 Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

Die Namensgebung in den ausgestellten Endanwenderzertifikaten muss dem X.500 Standard entsprechen. Weitere Namensformen sind darüber hinaus möglich.

3.1.2 Notwendigkeit für aussagefähige Namen

Eine **RfA** Sub-CA muss aussagekräftige Inhaber-Namen in ihrem eigenen Zertifikatsantrag und in den von ihr ausgestellten Endanwenderzertifikaten verwenden, um die Identität des Endnutzers oder -systems klar erkenntlich zu machen. Sie darf die Identität des Endnutzers oder -systems nicht verschleiern oder verbergen.

Für alle neuen **RfA**-Sub CAs muss aus dem Namen im Zertifikat der Name der Rundfunkanstalt, der Gemeinschaftseinrichtung oder Dritten[1] hervorgehen. Dabei muss im `subject` des Zertifikats in der CN-Komponente die Abkürzung der Rundfunkanstalt, Gemeinschaftseinrichtung oder von Dritten (z. B. BR-Sub-CA, MDR-User-CA, RB-Issuing-CA, ...), im O-Attribut der volle Name der Rundfunkanstalt und im C-Attribut „DE“ stehen. Falls es notwendig wird, für unterschiedliche Instanzen einer **RfA**-CA eindeutige Namen zu verwenden, bspw. im Zuge einer Migration, wird empfohlen, dem Namen das Jahr, in dem die betreffende CA-Instanz erstellt wird, oder eine fortlaufende Nummer (z. B. BR-CA02, SWR-CA02, ...) hintenanzustellen.

3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern

Es dürfen keine Pseudonyme verwendet werden, sondern die Zertifikate müssen eindeutig den Zertifikatsinhabern zugeordnet werden können.

Identifier, die über ein Managementsystem (bspw. ein MDM) verwaltet werden, fallen nicht unter Pseudonyme, selbst wenn sie ohne Hilfe des betreffenden Managementsystems nicht zugeordnet werden können.

Ein Wildcard-Zertifikat ist in Ausnahmefällen erlaubt, wenn das für eine dem Verwendungszweck entsprechende Subdomain vergeben wird (z.B. *.ad.rfa.de). Des Weiteren muss der Verwendungszweck/Begründung, Ausstellungsdatum und Ablaufdatum in Kapitel 10.2.2 des zugehörigen CPS-Dokuments dokumentiert werden.

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

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Die Distinguished Names im `subject`- und `issuer`-Feld des Zertifikats sollen den Zertifikatsinhaber und -herausgeber bezeichnen. Alternativ kann der Zertifikatsinhaber auch in der `SubjectAltName`-Erweiterung benannt werden. Diese `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 Vergabe von Namen muss sichergestellt sein, dass der Name innerhalb der ausstellenden CA eindeutig ist.

3.1.6 Anerkennung, Authentifizierung und Rolle von Markennamen

Keine Anforderungen.

3.2 Erstmalige Überprüfung der Identität

3.2.1 Methoden zur Überprüfung des Besitzes des privaten Schlüssels

Um sicherzustellen, dass der Antragsteller im Besitz des zugehörigen privaten Schlüssels ist, muss der Zertifikatsantrag (CSR) einer **RfA** Sub-CA mit ihrem privaten Schlüssel digital signiert sein. Ebenso darf eine **RfA** Sub-CA nur signierte Zertifikatsanträge akzeptieren und muss diese Signatur auf Gültigkeit und Korrektheit prüfen.

3.2.2 Authentifizierung von Organisationszugehörigkeiten

Beim Zertifikatsantrag durch eine **RfA** Sub-CA oder einen Endanwender muss keine Organisationszugehörigkeit überprüft werden.

3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikatsnehmers

Die Zertifikatsbeantragung bei einer **RfA** Sub-CA erfordert keine gesonderte Identitätsprüfung, wenn die Authentifizierung des Antragstellers auf Basis bereits erfasster Daten erfolgt. Ansonsten ist beim Neuantrag auf Zertifizierung eine gesonderte Identitätsprüfung des Antragstellers durchzuführen.

3.2.4 Ungeprüfte Zertifikatsnehmerangaben

RfA Sub-CAs dürfen keine ungeprüften Teilnehmerangaben in den Endanwenderzertifikaten aufnehmen. Bei automatisiert ausgestellten Zertifikaten (Auto Enrollment) ohne Prüfung des Zertifikatsantrags darf es nicht möglich sein, dass der Antragsteller einen Zertifikatsantrag manuell erstellt oder verändert.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Eine **RfA** Sub-CA darf Zertifikate nur nach Prüfung der Berechtigung des Antragstellers ausstellen. Hierbei kann die Berechtigungsprüfung eines Antragstellers automatisch und auch schon vorab erfolgen, so dass nur berechtigte Nutzer überhaupt einen Zertifikatsantrag stellen können. Der Prozess für die Prüfung der Berechtigung zur Antragsstellung muss von der **RfA** Sub-CA im einem CPS-Dokument dokumentiert werden.

3.2.6 Kriterien zur Zusammenarbeit

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

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, 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.

3.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen

Wurde das Zertifikat einer **RfA** Sub-CA gesperrt, 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.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Sperranträge dürfen von jedem gestellt werden.

Bei einem Sperrantrag für ein **RfA**-Endanwenderzertifikat ist keine gesonderte Identitätsprüfung durch die ausstellende **RfA** Sub-CA erforderlich, wenn der Antragsteller dem Betreiber der **RfA** Sub-CA persönlich bekannt ist. Ansonsten ist eine geeignete Identitätsprüfung des Antragstellers durchzuführen, die sich nach der Form des Sperrantrags richtet (Ausweisprüfung[2] bei persönlichem Sperrantrag, Rückruf bei telefonischem Sperrantrag von extern, Prüfung, ob der Anruf von einer Nebenstelle im Haus erfolgt, bei telefonischem Sperrantrag von intern, Nachfrage an die E-Mail Adresse des Antragstellers bei Sperrantrag per E-Mail).

[2] Der Ausweis muss mit einem Lichtbild ausgestattet sein.

4 Betriebsanforderungen

4.1 Zertifikatsantrag

4.1.1 Wer kann einen Zertifikatsantrag stellen?

Die Berechtigung, ein Zertifikat bei einer **RfA** Sub-CAs zu beantragen, haben alle natürlichen Personen, die freie oder feste Mitarbeiter der **RfA** sind bzw. im Auftrag der **RfA** arbeiten und Nutzer der **RfA** IT Infrastruktur sind (Zertifikatnehmer gemäß Abschnitt 1.3.3).

Die Beantragung von Systemzertifikaten kann bei vorhandenem AD-Konto durch das System selbst erfolgen. Andernfalls hat die Beantragung durch den verantwortlichen IT Administrator der **RfA** oder ein autorisiertes System (z.B. MDM-System) zu erfolgen.

4.1.2 Registrierungsprozess und Zuständigkeiten

Entweder wird das Schlüsselpaar zentral erzeugt oder der Antragsteller muss lokal ein Schlüsselpaar erzeugen und anschließend den öffentlichen Schlüssel gesichert in einem Zertifikatsantrag (CSR) bei der **RfA**-CA einreichen. Wird das Schlüsselpaar zentral erzeugt, muss dafür Sorge getragen werden, dass der private Schlüssel sicher an den Zertifikatsinhaber übermittelt wird. Die sichere Übermittlung muss beschrieben werden.

Endanwenderzertifikate dürfen entweder manuell oder automatisiert bei einer **RfA** Sub-CA beantragt werden. Sie sollen nach Möglichkeit automatisiert beantragt werden.

Zertifikatsanträge, bei denen der Name des Zertifikatsinhabers vom Antragsteller frei gewählt werden kann, erfordern eine Prüfung und Freigabe des Zertifikatsantrags durch einen **RfA** Sub-CA Certificate Manager, bevor das Zertifikat ausgestellt werden darf. Dies kann durch geeignete Mechanismen, wie ACME oder SCEP auch automatisiert erfolgen.

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Bei der Beantragung von Endanwenderzertifikaten ist keine gesonderte Identitätsprüfung erforderlich, wenn die Identitätsfeststellung auf andere Weise gesichert ist. Ansonsten ist beim Neuantrag auf Zertifizierung eine gesonderte Identitätsprüfung des Antragstellers durchzuführen. Diese ist zu dokumentieren.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Zertifikatsanträge für Endanwenderzertifikate sollen möglichst aus bereits erfassten Daten generiert werden, so dass die Zertifikate automatisiert ausgestellt werden können. Nur Zertifikatsanträge mit von Antragsteller selbst erfassten Daten – wie typischerweise bei SSL/TLS-Serverzertifikaten – müssen von den Betreibern einer **RfA** Sub-CA geprüft und angenommen oder bei Inkonsistenzen wie bspw. einem falschen Servernamen oder einer falschen IP-Adresse abgelehnt werden.

Die **RfA** Sub-CA muss in ihrem CPS-Dokument darlegen, welche Prüfungen sie bei Zertifikatsanträgen mit selbst erfassten Daten im Zertifikatsantrag durchführt und wann sie Zertifikatsanträge ablehnt.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Für **RfA** Sub-CAs gibt es keine Anforderungen an die Bearbeitungsdauer für Zertifikatsanträge für Endanwenderzertifikate.

4.3 Zertifikatsausgabe

4.3.1 Aktionen des Zertifizierungsdiensteanbieters bei der Ausgabe von Zertifikaten

Eine Ausgabe von Zertifikaten darf nur für gültige Zertifikatsanträge erfolgen, die syntaktisch korrekt sind und alle erforderlichen Informationen im Antrag enthalten. Die Aktionen bei der Zertifikatsausgabe müssen anhand der in dem CPS dokumentierten Prozesse erfolgen. Dabei muss sichergestellt sein, dass eine eindeutige Verbindung von Zertifikatsnehmer und dem zugehörigen Schlüsselpaar besteht.

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

RfA Sub-CAs müssen Zertifikatsnehmer nicht über ausgestellte Endanwenderzertifikate informieren.

4.4 Zertifikatsannahme

4.4.1 Verhalten für eine Zertifikatsannahme

Für die Endanwender ist kein dedizierter Prozess zur Zertifikatsannahme erforderlich.

4.4.2 Veröffentlichung des Zertifikats durch die CA

RfA Sub-CAs müssen ihrerseits ihr CA-Zertifikat so veröffentlichen, dass diese ARD-Netz-weit abgerufen werden können. Sollten zukünftig von einer **RfA** Sub-CA Verschlüsselungszertifikate für Benutzer ausgegeben werden, die von anderen Rundfunkanstalten genutzt werden, müssen diese ebenfalls im ARD-Netz veröffentlicht werden.

4.4.3 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe des Zertifikats

Für **RfA** Sub-CAs gibt es keine Anforderung bzgl. einer Benachrichtigung weiterer Zertifikatsinfrastruktur-Teilnehmer über die Ausstellung eines neuen Endanwenderzertifikats.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Die folgenden Anforderungen gelten sowohl für **RfA** Sub-CAs als auch für die von einer **RfA** Sub-CA zertifizierten Endanwender. Ein Zertifikatsnehmer (engl.: Subscribing Party) darf seinen Schlüssel und Zertifikat nur für die im Zertifikat genannten Verwendungszwecke einsetzen.

Die **RfA** Sub-CA muss Sorge tragen, dass ihr eigener privater Schlüssel angemessen gegen Diebstahl, Missbrauch und Verlust geschützt ist. Dies gilt auch für Backups des Systems und für eventuelle Sicherungskopien des Schlüssels. Sofern die **RfA** Sub-CA auf einem vernetzen IT-System betrieben wird, muss dies mit geeigneten Maßnahmen gegen Missbrauch geschützt und gehärtet sein. Dazu muss, wenn der private Schlüssel der **RfA**-CA in Software gespeichert wird, das Volume auf dem der private Schlüssel gespeichert ist hinreichend sicher (z. B. mit Bitlocker, VeraCrypt) verschlüsselt sein. Das gilt auch für Backups des Systems. Zum Schutz des privaten Schlüssels bei seiner Verwendung ist das System so nach einem anerkannten Härtungsstandard zu härten. In virtuellen Umgebungen ist zusätzlich eine wirksame Abschottung von anderen laufenden Prozessen notwendig. Der Einsatz eines kryptografischen Geräts, z. B. einer Smart Card oder von Hardware Security Moduls (HSM) zur Speicherung der privaten Schlüssel wird empfohlen. Die vernetzten Systeme sind mit geeigneten Maßnahmen gegen Missbrauch zu schützen. Die **RfA** Sub-CA muss die Maßnahmen für den angemessenen Schutz des privaten Schlüssels und des Systems in ihrem CPS dokumentieren.

Ein Zertifikatsnehmer muss Sorge tragen, dass sein privater Schlüssel angemessen vor Diebstahl, Missbrauch und Verlust geschützt ist und keiner unbefugten Person Zugang zum privaten Schlüssel gewährt wird. Das gilt auch für Backups der Schlüssel. Die Nutzung des Schlüssels und des Zertifikats ist nur in Übereinstimmung mit den Anforderungen in diesem Dokument zulässig.

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

Ein ursprünglich in Software erstelltes CA-Schlüsselpaar kann nachträglich in ein HSM verschoben werden und wird ab diesem Zeitpunkt als gleichwertig mit einem in Hardware erzeugten Schlüsselpaar angesehen, wenn die folgenden Bedingungen erfüllt sind:

- Das Schlüsselpaar wurde während seiner gesamten Lebenszeit gemäß den Anforderungen dieser Mindestanforderungen in der jeweils gültigen Version geschützt.
- Es sind keine Verdachtsmomente für eine Kompromittierung des Schlüssels bekannt.
- Unverzüglich nach dem Import in ein HSM werden alle Kopien des privaten Schlüssels (auch in Backups etc.) zuverlässig gelöscht. Über diese Löschung wird ein Protokoll angefertigt und bei der jeweiligen CA archiviert.

Bietet die **RfA**-CA bzw. **RfA** Sub-CA keine Möglichkeit der Schlüsselhinterlegung an oder wird eine optionale Schlüsselhinterlegungsmöglichkeit bei der **RfA**-CA bzw. **RfA** Sub-CA vom Zertifikatsnehmer nicht in Anspruch genommen, so ist der Zertifikatsnehmer selbst dafür zuständig, private Schlüssel so zu sichern, dass er ggf. verschlüsselte Daten wieder entschlüsseln kann. Eine **RfA** Sub-CA ist selbst dafür verantwortlich, dass sie ihre eigenen Schlüssel im Notfall wiederherstellen kann, um einen kontinuierlichen Zertifizierungsbetrieb zu gewährleisten.

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 in den Zertifikatserweiterungen `KeyUsage` und `ExtendedKeyUsage` genannten Verwendungszwecke akzeptieren.

4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüsselpaars (certificate renewal)

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

4.6.1 Bedingungen für eine Zertifikatserneuerung

Eine **RfA** Sub-CA muss eine Zertifikatserneuerung beantragen, wenn die Gültigkeit ihres Zertifikats abläuft und das CA-Zertifikat noch benötigt wird. In diesem Fall sollte eine Zertifikatserneuerung auch mit der Erzeugung von neuem Schlüsselmaterial verbunden sein. Die gleiche Empfehlung gilt auch für Endanwenderzertifikate. Zwingend erforderlich ist eine Schlüsselerneuerung jedoch nur, wenn das Zertifikat wegen Verdacht auf Kompromittierung des privaten Schlüssels gesperrt wurde oder wenn es den aktuellen kryptographischen Mindestanforderungen der Rundfunk-Root-CA nicht mehr genügt. Wenn die im Zertifikat enthaltenen Informationen unverändert bleiben, kann das bestehende Schlüsselmaterial beibehalten und nur das Zertifikat erneuert werden.

4.6.2 Wer darf eine Zertifikatserneuerung beantragen?

Eine Zertifikatserneuerung wird grundsätzlich durch den Zertifikatsnehmer bzw. eine autorisierte Person[1] beantragt. Es obliegt der zuständigen **RfA** Sub-CA, ob sie eine Zertifikatserneuerung aktiv unterstützt.

4.6.3 Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung

Der Prozess zur Bearbeitung eines Antrags auf Zertifikatserneuerung muss von einer **RfA** Sub-CA in ihrem CPS Dokument dokumentiert werden.

4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Keine weiteren Festlegungen.

4.6.5 Verhalten für die Annahme einer Zertifikatserneuerung

Keine weiteren Festlegungen.

4.6.6 Veröffentlichung der Zertifikatserneuerung durch die CA

Es gelten die gleichen Anforderungen wie bei einer Neubeantragung gemäß Abschnitt 4.4.2.

4.6.7 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Erneuerung des Zertifikats

Keine weiteren Festlegungen.

4.7 Zertifikatserneuerung mit Schlüsselerneuerung

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

[1] Bspw. für technische Funktionsaccounts, SSL/TLS- oder RADIUS-Server

4.7.1 Bedingungen für eine Zertifizierung nach Schlüsselerneuerung

Eine Zertifikatserneuerung mit Schlüsselwechsel kann beantragt werden, wenn z. B. die Gültigkeit eines Zertifikats abläuft. In diesem Fall könnte auch nur das Zertifikat erneuert, d. h. mit neuer Laufzeit wieder auf den gleichen öffentlichen Schlüssel ausgestellt werden (siehe Abschnitt 4.6).

Eine Zertifikaterneuerung mit Schlüsselwechsel muss zwingend beantragt werden, wenn ein Zertifikat aufgrund einer Schlüsselkompromittierung gesperrt wurde. Diese Anforderung muss von **RfA** Sub-CAs auch an ihre Endanwender gestellt werden.

4.7.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen?

Eine Schlüssel- und Zertifikatserneuerung muss grundsätzlich durch den Zertifikatsnehmer bzw. eine autorisierte Person/System[2] beantragt werden.

4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Der Prozess zur Bearbeitung eines Antrags auf Schlüssel- und Zertifikatserneuerung muss von jeder **RfA** Sub-CA im CPS Dokument dokumentiert sein.

4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

RfA Sub-CAs müssen ihre Zertifikatsnehmer nicht auf eine anstehende notwendige Zertifikatserneuerung aufmerksam machen und nicht über die Ausgabe eines Nachfolgezertifikats informieren.

4.7.5 Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen

Es gibt keine Anforderung an den Prozess zur Annahme des Zertifikats nach einer Schlüsselerneuerung.

4.7.6 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA

Es gelten die gleichen Anforderungen wie bei einer Neubeantragung gemäß Abschnitt 4.4.2.

4.7.7 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Keine Anforderung.

[2] Bspw. für technische Funktionsaccounts, SSL/TLS- oder RADIUS-Server

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. Bedingungen 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.

Technisch bedeutet dies die Sperrung des alten Zertifikats und die Ausstellung eines neuen Zertifikats.

4.8.2 Wer darf eine Zertifikatsänderung beantragen?

Eine Zertifikatsänderung darf grundsätzlich nur durch den Zertifikatsnehmer bzw. stellvertretend durch eine autorisierte Person/System[3] beantragt werden.

4.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung

Der Prozess zur Bearbeitung eines Antrags auf Zertifikatserneuerung muss von jeder **RfA** Sub-CA im CPS Dokument dokumentiert sein.

4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

RfA Sub-CAs müssen ihre Zertifikatsnehmer nicht über die Ausgabe eines neuen Zertifikats benachrichtigen.

4.8.5 Verhalten für die Annahme einer Zertifikatsänderung

Es gibt keine Anforderung an den Prozess zur Annahme einer Zertifikatsänderung.

4.8.6 Veröffentlichung der Zertifikatsänderung durch die CA

Es gelten die gleichen Anforderungen wie bei einer Neubeantragung gemäß Abschnitt 4.4.2.

[3] Bspw. für technische Funktionsaccounts, SSL/TLS- oder RADIUS-Server

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

Für **RfA** Sub-CAs gibt es keine Anforderung bzgl. einer Benachrichtigung weiterer Zertifikatsinfrastruktur-Teilnehmer.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Bedingungen für eine Sperrung

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

- Das Zertifikat enthält Angaben, die nicht gültig sind.
- Der private Schlüssel des Zertifikatsnehmers wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
- Der Zertifikatsnehmer ist nicht mehr berechtigt, das Zertifikat zu nutzen.
- Der Zertifikatsnehmer hält die CP nicht ein.
- Die zuständige **RfA** Sub-CA hält die CP oder das CPS nicht ein.
- Die **RfA** Sub-CA oder die **RfA**-CA stellt den Zertifizierungsbetrieb ein.
- Der Zertifikatsnehmer benötigt das Zertifikat nicht mehr.

4.9.2 Wer kann eine Sperrung beantragen?

Sperranträge dürfen von jedem eingereicht werden.

4.9.3 Verfahren für einen Sperrantrag

Das Verfahren und die Berechtigung für die Beantragung einer Zertifikatssperrung muss von einer **RfA** Sub-CA in einem CPS Dokument dokumentiert und ihren Zertifikatsnehmern bekannt gegeben werden.

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 RfA-CA

Eine Zertifikatssperrung muss unverzüglich erfolgen.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Eine **RfA** Sub-CA muss den Zertifikatsprüfern RfA-übergreifend, d. h. mindestens intern und im ARD-Netz Sperrinformationen zu ihren ausgestellten Zertifikaten zur Verfügung stellen. Hierzu können Sperrlisten oder OCSP-Responder eingesetzt werden.

4.9.7 Frequenz der Veröffentlichung von Sperrlisten

Die Sperrliste einer **RfA** Sub-CA darf maximal acht Tage gültig sein. Es ist mindestens wöchentlich (alle sieben Tage) eine neue Sperrliste zu erstellen. Im Falle einer Sperrung eines Zertifikats muss zusätzlich eine neue Sperrliste ausgestellt und veröffentlicht werden die ebenfalls wieder maximal acht Tage gültig sein darf.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die maximale Latenzzeit für Sperrlisten darf bei **RfA** 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-Sperrinformationen

An **RfA** Sub-CAs bestehen keine Anforderungen nach einem Online-Dienst zur Auskunft der Gültigkeit der von ihr ausgestellten Zertifikate. Sie kann jedoch im eigenen Ermessen einen solchen OCSP-Dienst zusätzlich oder alternativ zur Verwendung von Sperrlisten anbieten.

4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen

Keine Anforderungen.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

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

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Bei Kompromittierung des privaten Schlüssels einer **RfA** Sub-CA, eines Endnutzers oder Systems muss das zugehörige Zertifikat unverzüglich nach Bekanntwerden der Kompromittierung oder eines hinreichenden Verdachts hierauf gesperrt werden.

4.9.13 Bedingungen für eine Suspendierung

Eine temporäre Sperrung bzw. eine Suspendierung von Zertifikaten ist 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

An eine **RfA** Sub-CAs besteht keine Anforderung nach einem Statusabfragedienst der von ihr ausgestellten Zertifikate. Sie kann jedoch im eigenen Ermessen einen solchen OCSP-Dienst zusätzlich oder alternativ zur Verwendung von Sperrlisten anbieten (siehe Abschnitt 4.9.9).

4.10.1 Funktionsweise des Statusabfragedienstes

Keine Anforderung (s.o.).

4.10.2 Verfügbarkeit des Statusabfragedienstes

Keine Anforderung (s.o.).

4.10.3 Optionale Leistungen

Keine Anforderung (s.o.).

4.11 Kündigung durch den Zertifikatsnehmer

Im Fall einer Kündigung durch den Zertifikatsnehmer muss das Zertifikat gesperrt werden.

4.12 Schlüsselhinterlegung und Wiederherstellung

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel

Bietet eine **RfA** Sub-CA eine Schlüsselhinterlegung – d. h. in diesem Zusammenhang die treuhänderische zentrale Verwahrung des privaten Schlüssels zu einem Zertifikat, die sie erstellt hat, als Notfallvorsorge für den Zertifikats- und Schlüsselinhaber – an, muss sie die Verfahren und Prozesse der Schlüsselhinterlegung im 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.

Die Sicherung eines Schlüssels durch den Schlüsselinhaber selbst oder ein Backup der Systeme, auf denen der Schlüssel für seine beabsichtigte Nutzung gespeichert ist, stellen keine Schlüsselhinterlegung im Sinne dieser Regelung dar.

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Keine Anforderungen.

5 Nicht-technische Sicherheitsmaßnahmen

Die Gewährleistung geeigneter infrastruktureller, organisatorischer und personeller Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb der **RfA**-CA und untergeordneter **RfA** Sub-CAs. Mindestanforderungen an diese Sicherheitsmaßnahmen für untergeordnete **RfA** Sub-CAs werden nachfolgend beschrieben. Detaillierte Informationen sollten von der **RfA** Sub-CA in einem Sicherheitskonzept festgeschrieben werden. Dieses muss nicht veröffentlicht werden.

5.1 Bauliche Sicherheitsmaßnahmen

5.1.1 Lage und Gebäude

Der Serverraum, in dem eine **RfA** Sub-CA betrieben wird, muss durch geeignete physische Sicherheitsvorkehrungen einen ausreichenden Schutz vor äußeren Einflüssen garantieren.

5.1.2 Zugang

Der Zutritt zu den Betriebsräumen der **RfA** Sub-CAs muss durch geeignete technische und infrastrukturelle Maßnahmen gesichert und darf nur autorisierten Mitarbeitern gestattet werden. Der Zutritt durch betriebsfremde Personen muss durch eine Besucherregelung festgelegt werden. Die Maßnahmen zur Sicherung des Zutritts und die Besucherregelung müssen im CPS-Dokument beschrieben werden.

5.1.3 Strom, Heizung und Klimaanlage

Stromversorgung und ausreichende Klimatisierung müssen im Serverraum, in dem eine **RfA** Sub-CA betrieben wird, durch geeignete Maßnahmen sichergestellt sein.

5.1.4 Wassergefährdung

Gefährdungen durch Wasser müssen hinreichend ausgeschlossen sein.

5.1.5 Brandschutz

Im Serverraum ist ein geeigneter Brandschutz vorzusehen.

5.1.6 Lager und Archiv

Datenträger mit sicherheitsrelevanten, vertraulichen oder personenbezogenen Daten müssen vor unberechtigten Zugriffen geschützt aufbewahrt werden.

5.1.7 Datenvernichtung

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

5.1.8 Disaster Backup

Zu Disaster-Recovery-Zwecken muss das jeweils neuste komplette System-Backup der **RfA** Sub-CA, eine Sicherheitskopie der **RfA** Sub-CA Schlüssel und der zugehörige Passwortbrief sicher aufbewahrt werden.

5.2 Verfahrensvorschriften

5.2.1 Rollenkonzept

Für Installation, Konfiguration, Betrieb und Wiederherstellung aus dem Backup der **RfA** Sub-CA sind geeignete Rollen zu definieren und umzusetzen.

5.2.2 Mehraugenprinzip

Nur das optional mögliche Key-Recovery von Verschlüsselungsschlüsseln benötigt ein Vier-Augen-Prinzip sofern dieses nicht durch den Benutzer selbst durchgeführt wird.

5.2.3 Identifizierung und Authentifizierung jeder Rolle

Zur Authentifizierung bei allen Rollen genügt eine Ein-Faktor-Authentifizierung, wie bspw. Benutzername und Passwort.

5.2.4 Rollentrennung

Keine der Rollen erfordert eine Aufgabentrennung.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

Die CA-Administratoren der **RfA** Sub-CA müssen den Stand der Technik und die Best Practices im Bereich Zertifikatsinfrastruktur kennen.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Eine Sicherheitsüberprüfung der CA-Administratoren ist nicht erforderlich.

5.3.3 Anforderungen an Schulungen

Für CA-Administratoren einer **RfA** Sub-CA bestehen keine Anforderungen an bestimmte Schulungen.

5.3.4 Häufigkeit von Schulungen und Belehrungen

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

5.3.5 Häufigkeit und Folge von Job-Rotation

Keine Anforderungen.

5.3.6 Maßnahmen bei unerlaubten Handlungen

Keine Anforderungen.

5.3.7 Anforderungen an freie Mitarbeiter

Keine Anforderungen.

5.3.8 Dokumente, die dem Personal zur Verfügung gestellt werden müssen

Den CA-Administratoren einer **RfA** Sub-CA muss dieses Dokument sowie die CP und CPS der **RfA**-CA zur Verfügung gestellt werden.

5.4 Überwachungsmaßnahmen

5.4.1 Arten von aufgezeichneten Ereignissen

Alle sicherheitsrelevanten Ereignisse einer **RfA** Sub-CA müssen in Log-Dateien protokolliert werden. Zu den sicherheitsrelevanten Ereignissen zählen insbesondere:

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

5.4.2 Häufigkeit der Bearbeitung der Aufzeichnungen

Nur bei Verdachtsmomenten ist eine Prüfung der Log-Protokolle (Aufzeichnungen) erforderlich.

5.4.3 Aufbewahrungszeit von Aufzeichnungen

Das Log-Protokoll (Aufzeichnungen) einer **RfA** Sub-CA muss für mindestens sieben Tage aufbewahrt werden.

5.4.4 Sicherung der Aufzeichnungen

Die Protokolldaten (Aufzeichnungen) müssen gegen unberechtigten Zugriff, Löschung und Manipulation geschützt werden.

5.4.5 Datensicherung der Aufzeichnungen

Das Log-Protokoll (Aufzeichnungen) einer **RfA** Sub-CA ist regelmäßig zu sichern.

5.4.6 Speicherung der Aufzeichnungen (intern / extern)

Keine Anforderungen.

5.4.7 Benachrichtigung der Ereignisauslöser

Keine Anforderungen.

5.4.8 Schwachstellenanalyse

Bei Online-CAs muss die Software einer **RfA** Sub-CA in das Patch-Management der **RfA** aufgenommen werden. Schwachstellen bei den eingesetzten Systemen sind nach Bekanntwerden der Schwachstelle und Vorliegen eines Patches umgehend zu schließen.

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen

Es bestehen an **RfA** Sub-CAs keine Anforderungen für aufzubewahrende Aufzeichnungen. Es wird empfohlen eine Sicherungskopie des privaten CA-Schlüssels, das Zertifikat und das Passwort für den archivierten CA-Schlüssel zu sichern. Über die Archivierung von Zertifikats-, Sperranträgen, Log-Dateien, etc. entscheidet jede **RfA** Sub-CA abhängig von den Anforderungen der von ihr unterstützten Anwendungen.

5.5.2 Aufbewahrungsfristen für archivierte Daten

Wenn der CA-Schlüssel und das CA-Zertifikat sowie das hinterlegte Passwort gesichert werden, sollten diese während der gesamten Verwendungsdauer des privaten **RfA** Sub-CA-Schlüssels aufbewahrt werden.

5.5.3 Sicherung des Archivs

Wenn der CA-Schlüssel und das CA-Zertifikat sowie das Passwort für die Sicherungskopie gesichert werden, müssen die Sicherungskopie des CA-Schlüssels sowie das Passwort vor unberechtigtem Zugriff geschützt verwahrt werden.

5.5.4 Datensicherung des Archivs

Keine Anforderungen.

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

Keine Anforderungen.

5.5.6 Archivierung (intern / extern)

Keine Anforderungen.

5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen

Keine Anforderungen.

5.6 Schlüsselwechsel der RfA-CA

Der private Schlüssel einer **RfA** Sub-CA darf nur so lange zum Ausstellen von Zertifikaten eingesetzt werden, wie die Gültigkeit der untergeordneten Zertifikate noch innerhalb des Gültigkeitsrahmens des **RfA** Sub-CA Zertifikats liegt. Beim Schlüsselwechsel einer **RfA** Sub-CA muss kein neues Schlüsselmaterial generiert werden.

5.7 Kompromittierung und Geschäftsweiterführung bei der RfA-CA

5.7.1 Behandlung von Vorfällen und Kompromittierungen

Bei Verlust eines Schlüssels einer **RfA** Sub-CA durch Systemausfall oder Löschung der Daten sollte der CA Schlüssel aus einer Sicherungskopie wiederhergestellt werden können.

Falls im Laufe der Gültigkeitsdauer eines **RfA** Sub-CA Zertifikats die verwendeten Kryptoverfahren bzw. Schlüssellängen (siehe Abschnitt 6.1 und 7.1) nicht mehr als hinreichend sicher zu betrachten sind, müssen der IT-Sicherheitsbeauftragte der **RfA** und die CA-Steuerungsgruppe informiert werden, welche über die nächsten Schritte entscheiden.

5.7.2 Rechnerressourcen-, Software- und/oder Datenkompromittierung

Im Verdachtsfall von kompromittierter Software oder Daten sind die Daten aus einer unkompromittierten Datensicherung zurück zu spielen. 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 RfA-CA

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

5.7.4 Möglichkeiten zur Geschäftsweiterführung nach einer Kompromittierung

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

5.8 Schließung einer RfA-CA oder einer Registrierungsstelle

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

6 Technische Sicherheitsmaßnahmen

Die Gewährleistung geeigneter technischer Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb einer Zertifikatsinfrastruktur. Nachfolgend werden Mindestanforderungen an technische Sicherheitsmaßnahmen für **RfA** Sub-CAs beschrieben. Die Umsetzung dieser Anforderungen muss in einem CPS für die **RfA** Sub-CAs beschrieben werden.

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

Das Schüsselpaar einer **RfA** Sub-CA kann in Software oder Hardware erzeugt und gespeichert werden. Für RAs kann eine Schlüsselerzeugung bei der RA oder der zugehörigen **RfA** Sub-CA durchgeführt werden. Wird der Schlüssel bei einer **RfA** Sub-CA zentral erzeugt, ist das Verfahren im CPS Dokument der **RfA** Sub-CA darzulegen.

Für Endanwender kann die Schlüsselerzeugung durch diesen selbst oder bei der zugehörigen RA oder einer **RfA** Sub-CA durchgeführt werden. Wird der Schlüssel bei der RA oder einer **RfA** Sub-CA zentral erzeugt, ist das Verfahren im CPS Dokument der **RfA** Sub-CA darzulegen.

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Ist eine Übermittlung des privaten Schlüssels an einen Zertifikatsnehmer oder eine RA notwendig, so ist der private Schlüssel während der Übermittlung ausreichend zu sichern und das Verfahren im CPS Dokument der **RfA** Sub-CA darzulegen.

6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

Der öffentliche Schlüssel der Endanwender muss per HTTPS, per E-Mail oder auf einem Datenträger an die **RfA** Sub-CA übermittelt werden.

6.1.4 Lieferung öffentlicher Schlüssel der RfA-CA an Zertifikatsnutzer

RfA Sub-CAs müssen ihr eigenes Sub-CA-Zertifikat den Zertifikatsprüfern im AD, LAN, ARD-Netz und bei Bedarf auch im Internet zur Verfügung stellen, so dass es automatisch von einer Anwendung zu Verifikationszwecken heruntergeladen und verwendet werden kann.

6.1.5 Schlüssellängen

RSA

Das Schlüsselpaar einer **RfA** Sub-CA muss eine Schlüssellänge von mindestens 4096 Bit aufweisen. Die Schlüsselpaare der Endnutzer oder -systeme müssen mindestens 4096 Bit lang sein. Bei Systemen, bei denen eine Schlüssellänge von 4096 Bit technisch nicht möglich ist, dürfen noch Schlüssel von einer Länge von 2048 Bit genutzt werden.

Elliptische Kurven

Alternativ zu RSA dürfen Endanwenderzertifikate auch für Schlüssel auf Basis elliptischer Kurven ausgestellt werden. In diesem Fall ist die Nutzung der folgenden Kurven zulässig:

- NIST P-256
- *NIST P-384*
- *NIST P-521*

Hinweis: *Die Nutzung von Kurven außerhalb der NIST P-256 ist derzeit noch nicht final freigegeben.*

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 einer **RfA** Sub-CA müssen den Anforderungen aus FIPS 140-2 oder einem vergleichbaren Standard entsprechen.

6.1.7 Schlüsselverwendungen

Alle von der **RfA** Sub-CAs ausgestellten Zertifikate für Endanwender oder Systeme sowie die zugehörigen privaten Schlüssel dürfen nur zu den in den Zertifikaten spezifizierten Verwendungszwecken eingesetzt werden.

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

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

Die Schlüsselerzeugung einer **RfA** Sub-CA, eines Endanwenders oder Systems kann auf einer Smartcard, einem HSM (auch TPM) oder softwarebasiert auf dem Rechner der **RfA** Sub-CA, des Endanwen-

ders oder Systems erfolgen.

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

Der private Schlüssel einer **RfA** Sub-CA, eines Endanwenders oder Systems kann, muss aber nicht, auf mehrere Personen aufgeteilt sein.

6.2.3 Hinterlegung privater Schlüssel

Bietet eine **RfA** Sub-CA eine Schlüsselhinterlegung an, muss sie die Verfahren und Prozesse der Schlüsselhinterlegung im CPS Dokument dokumentieren. Diese müssen der eigenen Sicherheitsrichtlinie und dem aktuellen Stand der Technik entsprechen. Eine Schlüsselhinterlegung darf nicht für Authentisierungsschlüssel und Signaturschlüssel von Benutzern erfolgen.

6.2.4 Sicherung privater Schlüssel

Die privaten Schlüssel von **RfA** Sub-CAs, Endanwendern und Systemen können, müssen aber nicht, zentral gesichert werden. Schlüssel, die zur Authentisierung oder Signatur genutzt werden, dürfen nicht zentral hinterlegt werden.

6.2.5 Archivierung privater Schlüssel

Der private Schlüssel einer **RfA** Sub-CA kann, muss aber nicht, archiviert werden. Falls er archiviert wird, müssen die Sicherungskopie und das zugehörige Passwort vor unberechtigtem Zugriff geschützt verwahrt werden.

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Keine Anforderung.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

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

6.2.8 Aktivierung privater Schlüssel

Der private Schlüssel einer **RfA** Sub-CA muss vor unautorisiertem Zugriff geschützt werden. Die privaten Schlüssel der Endanwender müssen durch ein geeignetes Passwort vor unautorisiertem Zugriff geschützt werden. Der Zugriff auf den privaten Schlüssel von Systemen hingegen muss nicht

zwingend durch ein Passwort gesichert sein. Dafür muss aber der Zugriff auf die Systeme hinreichend gesichert werden.

6.2.9 Deaktivierung privater Schlüssel

Der private Schlüssel einer **RfA** Sub-CA muss deaktiviert werden können, ggf. durch Ziehen der Smartcard aus dem Kartenleser oder durch Beendigung des CA-Programms bzw. Zertifikatsdienstes. Ein Endanwender muss ebenfalls die Möglichkeit haben, seinen privaten Schlüssel zu deaktivieren. Auch für Systeme muss der private Schlüssel deaktiviert werden können.

6.2.10 Zerstörung privater Schlüssel

Private Schlüssel, die in Software gespeichert sind, müssen mit geeigneten Lösch-Tools sicher gelöscht werden. Um den privaten Schlüssel auf einer Smartcard zu löschen, muss diese physisch zerstört werden. Die Vernichtung von privaten Schlüsseln muss auch die Sicherungskopien sowie alle weiteren Datenspeicher, die den privaten Schlüssel enthalten können (VMware-Snapshots, Backups, SAN-Snapshots) mit einschließen. Sofern bei Endanwenderzertifikaten der zugehörige Schlüssel nicht zuverlässig vernichtet werden kann (bspw. bei Zertifikaten auf verloren gegangenen Geräten) muss sichergestellt werden, dass das betreffende Zertifikat unverzüglich gesperrt wird.

6.2.11 Beurteilung kryptographischer Module

Keine Anforderung.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Keine Anforderung.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Ein **RfA** Sub-CA Zertifikat darf für maximal 10 Jahre ausgestellt werden. Der private Schlüssel einer **RfA** Sub-CA darf nur solange zur Ausstellung von Endanwenderzertifikaten verwendet werden, wie das Gültigkeitsende der ausgestellten Zertifikate noch im Gültigkeitsbereich der **RfA** Sub-CA liegt. Endanwenderzertifikate dürfen eine maximale Laufzeit von fünf Jahren haben. OCSP-Signing-Zertifikate dürfen eine maximale Laufzeit von 30 Tagen haben.

6.4 Aktivierungsdaten

6.4.1 Aktivierungsdaten

Der CA-Administrator der **RfA** Sub-CA muss ein ausreichend sicheres Passwort zur Anmeldung an die **RfA** Sub-CA festlegen. Bei der Benutzung von Smartcards muss zusätzlich eine sichere PIN verwendet werden.

6.4.2 Schutz von Aktivierungsdaten

Das Passwort bzw. die PIN beim Einsatz von Smartcards der **RfA** Sub-CA darf nur dem CA-Administrator bekannt sein.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Bei Online-CAs ist die **RfA** Sub-CA auf Basis eines gehärteten Betriebssystems zu betreiben und durch Benutzerauthentisierung und Zugriffskontrolle vor unberechtigten Zugriffen zu schützen. Sämtliche nicht benötigten Netzdienste müssen deaktiviert werden.

6.5.2 Beurteilung von Computersicherheit

Keine Anforderung.

6.6 Technische Maßnahmen während des Life Cycles

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

Keine Anforderung.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Bei Online-CAs müssen aktuelle Updates und Patches für die Systeme der **RfA** Sub-CA nach einem definierten Schema der jeweiligen RfA (bspw. beim nächsten Wartungsfenster) eingespielt werden. Sicherheitskritische Patches ab einer CVSS Schachstellen-Bewertung von 7.0 oder höher müssen umgehend eingespielt werden.

6.6.3 Sicherheitsmaßnahmen während der Life Cycles

Keine Anforderung.

6.7 Sicherheitsmaßnahmen für Netze

Der Server einer Sub-CA muss geeignet vor unberechtigten Zugriffen per Netzwerk und vor Zugriffen von außen geschützt sein. Jede Sub-CA muss in ihrem CPS die Sicherheitsmaßnahmen für das Netzwerk beschreiben.

6.8 Zeitstempel

Keine Anforderung.

7 Profile von Zertifikaten, Sperrlisten und OCSP

7.1 Zertifikatsprofile

7.1.1 Versionsnummern

Die Versionsnummer im Zertifikat muss auf Version 3 (= Wert 2) gesetzt werden. Dieser Wert kennzeichnet X.509 Zertifikate mit Erweiterungen.

7.1.2 Zertifikatserweiterungen

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

- `KeyUsage` (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` (Zugriff auf Stelleninformationen), `ExtendedKeyUsage` (Erweiterte Schlüsselverwendung) oder `CertificatePolices` (Zertifikatrichtlinien).

Sofern eine **RfA** Sub-CA OCSP anbietet, braucht in Zertifikaten für OCSP-Signing die Erweiterung `CRLDistributionPoints` nicht enthalten zu sein.

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) eine einheitliche „Erweiterte Schlüsselverwendung“ (X509 v3, `Extended Key Usage`) mit der Objektkennung (`Object Identifier`) `1.3.6.1.4.1.42638.2.1` enthalten sein.

Die Erweiterung soll als nicht-kritisch markiert werden. Es dürfen nur Maschinenzertifikate für WLAN genutzt und mit dieser Objektkennung in der `ExtendedKeyUsage` versehen werden.

Um weConnect-Zertifikate RfA-übergreifend einheitlich zu kennzeichnen, muss in allen weConnect-Zertifikate eine einheitliche „Erweiterte Schlüsselverwendung“ (X509 v3, `Extended Key Usage`) mit der Objektkennung (`Object Identifier`) `1.3.6.1.4.1.42638.2.2` enthalten sein.

7.1.3 Algorithmen OIDs

Zur Signatur von Zertifikaten wird bis auf weiteres der Algorithmus „sha256WithRSAEncryption“ verwendet. Als Algorithmen-Identifier für den Subject Public Key (Teilnehmerschlüssel) in CA-Zertifikaten und Endanwenderzertifikaten wird bis auf weiteres der folgende genutzt:

- rsaEncryption (OID: `1.2.840.113549.1.1.1`)

In Endanwenderzertifikaten alternativ auch:

- id-ecPublicKey (OID: `1.2.840.10045.2.1`)

Zu den OIDs der zulässigen elliptischen Kurven siehe Kapitel 6.1.6.

7.1.4 Namensformate

Siehe Kapitel 3.1.4.

7.1.5 Namensbeschränkungen

Keine Anforderung.

7.1.6 OIDs der Zertifikatsrichtlinien

Zur RfA-übergreifenden Kennzeichnung von WLAN-Zertifikaten müssen diese eine einheitliche „Erweiterte Schlüsselverwendung“ (X509 v3, `Extended Key Usage`) mit der Objektkennung (`Object Identifier`) `1.3.6.1.4.1.42638.2.1` enthalten, siehe Abschnitt 7.1.2.

Zur RFA-übergreifenden Kennzeichnung von weConnect-Zertifikaten müssen diese einen einheitlichen OID Key-Purpose-Identifier in der „Erweiterte Schlüsselverwendung“ (X509 v3, `Extended Key Usage`) Erweiterung enthalten, siehe Abschnitt 7.1.2.

Zusätzlich kann eine **RfA** Sub-CA in der CertificatePolicies Erweiterung in den ausgestellten Endanwenderzertifikaten ihre Policy über eine zugeordnete OID referenzieren.

Policy-Dokumente (bzw. deren neue Versionen) der teilnehmenden Rundfunkanstalten, die ab dem 01.02.2022 der Rundfunk-Root-CA vorgelegt und im ARD-Netz veröffentlicht werden, erhalten zur Kennzeichnung eine OID unterhalb des OID-Präfixes der Rundfunk-Root-CA (`1.3.6.1.4.1.42638`).

Eine RfA darf eigene OIDs ergänzend zu den nach diesen Mindestanforderungen verlangten OIDs der Rundfunk-Root-CA verwenden.

7.1.7 Nutzung der Erweiterung ”Policy Constraints”

Keine Anforderung.

7.1.8 Syntax und Semantik von ”Policy Qualifiers”

Keine Anforderung.

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung Zertifikatsrichtlinie

Keine Anforderung.

7.2 Sperrlistenprofile

7.2.1 Versionsnummer(n)

Die Versionsnummer der Sperrliste muss auf Version 2 (= Wert 1) gesetzt werden. Dieser Wert kennzeichnet X.509 Sperrlisten mit Erweiterungen.

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

In den Sperrlisten der **RfA** Sub-CAs müssen mindestens folgende Erweiterungen enthalten sein:

- AuthorityKeyIdentifier (Stellenschlüsselkennung)
- CRLNumber (Sperrlistennummer)

Diese Sperrlistenerweiterungen müssen alle als nicht kritisch markiert werden. Optional dürfen weitere nicht kritische Erweiterungen in den Sperrlisten der **RfA** Sub-CA ergänzt werden.

7.3 Profile des Statusabfragedienstes (OCSP)

7.3.1 Versionsnummer(n)

Keine Anforderung.

7.3.2 OCSP Erweiterungen

Keine Anforderung.

8 Überprüfungen und andere Bewertungen

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

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

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

Die Ergebnisse dieser Überprüfung finden Eingang in den Jahresbericht.

9 Andere finanzielle und rechtliche Angelegenheiten

9.1 Preise

Keine Anforderung.

9.2 Finanzielle Zuständigkeiten

Keine Anforderung.

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, müssen als vertrauliche Informationen eingestuft und behandelt werden.

9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören

Alle Informationen, die in den veröffentlichten Zertifikaten und Sperrlisten einer **RfA** Sub-CA enthalten sind oder davon abgeleitet werden können, müssen nicht als vertraulich eingestuft werden.

9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen

Jede von der **RfA**-CA zertifizierte **RfA** Sub-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.

9.4 Datenschutz von Personendaten

9.4.1 Datenschutzkonzept

Die von der **RfA**-CA zertifizierten **RfA** Sub-CAs und RAs müssen zur Leistungserbringung personenbezogene Daten elektronisch speichern und verarbeiten. Dies muss in Übereinstimmung mit den entsprechenden Gesetzen geschehen.

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 einer **RfA** Sub-CA muss der Nutzung von personenbezogenen Daten durch die **RfA** Sub-CA zustimmen, 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 **RfA**-CA zertifizierten **RfA** Sub-CAs unterliegen dem Recht des jeweiligen Staates 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 **RfA**-CA ist Urheber des vorliegenden Dokuments. Eine Weitergabe von veränderten Fassungen dieser CP ist ohne Zustimmung von dem Betreiber der **RfA**-CA nicht zulässig.

9.6 Zusicherungen und Garantien

9.6.1 Zusicherungen und Garantien der CA

Jede von der **RfA**-CA zertifizierte **RfA** Sub-CAs muss die Anforderungen dieses Policy-Dokuments geeignet umsetzen und ihre Aufgaben nach bestem Wissen und Gewissen durchführen.

9.6.2 Zusicherungen und Garantien der RA

Jede RA muss die Anforderungen dieses Policy-Dokuments geeignet umsetzen und ihre Aufgaben nach bestem Wissen und Gewissen durchführen.

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

Sofern weitere Teilnehmer als Dienstleister in den Zertifizierungsprozess eingebunden werden, muss der beauftragte Dienstleister zur Einhaltung dieser CP und CPS verpflichtet werden.

9.7 Haftungsausschlüsse

Keine Anforderung.

9.8 Haftungsbeschränkungen

Keine Anforderung.

9.9 Schadensersatz

Keine Anforderung.

9.10 Gültigkeitsdauer und Beendigung

9.10.1 Gültigkeitsdauer

Keine Anforderung.

9.10.2 Beendigung

Keine Anforderung.

9.10.3 Auswirkung der Beendigung und Weiterbestehen

Von der Aufhebung einer **RfA** Sub-CA Policy unberührt bleibt die Verantwortung des Betreibers zum Schutz vertraulicher Informationen und personenbezogener Daten.

9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern

Keine Anforderung.

9.12 Ergänzungen

9.12.1 Verfahren für Ergänzungen

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

9.12.2 Benachrichtigungsmechanismen und -fristen

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

Bei Änderung von Anforderungen in einem Policy-Dokument einer **RfA** Sub-CA müssen die Endanwender innerhalb eines Monats von der **RfA** Sub-CA informiert werden.

9.12.3 Bedingungen für OID Änderungen

Wenn eine **RfA** Sub-CA ihr Policy-Dokument über einen OID kennzeichnet und es werden Änderungen in diesem Policy-Dokument vorgenommen, die sicherheitsrelevante oder andere substanzielle Aspekte betreffen, ist eine Änderung der OID dieses Dokuments erforderlich. Wenn zusätzlich der OID zur Identifikation des Policy-Dokuments in der certificatePolices Erweiterung der ausgestellten Endanwenderzertifikate enthalten ist, müssen zukünftig alle von der betreffenden **RfA** Sub-CA ausgestellten Zertifikate diese neue OID der geänderten Policy enthalten.

9.13 Verfahren zur Schlichtung von Streitfällen

Keine Anforderung.

9.14 Zugrundeliegendes Recht

Der Betrieb der **RfA**-CA unterliegt den Gesetzen des jeweiligen Staates.

9.15 Einhaltung geltenden Rechts

Eine **RfA** Sub-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 dieses Policy-Dokuments ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2 Abgrenzungen

Keine Anforderung.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Mindestanforderungen 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)

Keine Anforderung.

9.16.5 Höhere Gewalt

Keine Anforderung.

9.17 Andere Bestimmungen

Keine Anforderung.