CPS Online BR Sub-CA

Inhaltsverzeichnis

1 Einleitung

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

RfA-CA wird als Synonym für die BR-CA verwendet, **RfA Issuing-CA** für die BR-Sub-CA-2032

1.1 Überblick

Dieses Dokument ist das Certificate Practice Statement (CPS) der **RfA Issuing-CA**. Es stellt dar, wie die Mindestanforderungen der Rundfunk-Root-CA und die Vorgaben der Certificate Policy (CP) der **RfA**-CA für untergeordnete CAs durch die **RfA Issuing-CA** umgesetzt werden.

Alle in den Mindestanforderungen der Rundfunk-Root-CA und der Certificate Policy (CP) der **RfA**-CA für untergeordnete CAs beschriebenen Verfahren sowie Anforderungen an Endzertifikate und deren Zertifikatsnehmer sind für **RfA Issuing-CAs** verbindlich und können nicht abgeschwächt werden. Die Verfahren und Anforderungen betreffen die infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen und Abläufe innerhalb der **RfA Issuing-CA** und legen dabei insbesondere die Rahmenbedingungen für die Ausstellung von Zertifikaten entsprechend der internationalen Norm X.509 fest.

1.2 Name und Kennzeichnung des Dokuments

Name: Regelungen für den Zertifizierungsbetrieb (CPS) der BR-Sub-CA-2032

Version: 1.0

Datum: 02.07.2024

OID: 1.3.6.1.4.1.42638.1.4.3.1

1.3 Zertifikatsinfrastruktur-Teilnehmer

1.3.1 Zertifizierungsstellen

Die **RfA** betreibt die unteren beiden Stufen einer dreistufige Zertifikatsinfrastruktur-Hierarchie:

- Den Vertrauensanker der Zertifikatsinfrastruktur bildet die vom ARD-Sternpunkt betriebene Rundfunk-Root-CA.
- Die Rundfunk-Root-CA zertifiziert die **RfA**-CA. Die **RfA**-CA stellt ausschließlich Sub-CA Zertifikate aus.
- Die **RfA**-CA zertifiziert die **RfA Issuing-CA**. Die **RfA Issuing-CA** stellt ausschließlich Endanwenderzertifikate aus.

Die **RfA Issuing-CA** wird unter Nutzung der Microsoft Active Directory Certificate Services in einer Virtuellen Maschine (VM) unter Windows Server 2022 betrieben.

1.3.2 Registrierungsstellen

Die **RfA-Issuing-CA** nutzt eine oder mehrere Registrierungsstellen (RA) zur Überprüfung der Identität und Authentizität von Zertifikatsnehmern, sofern eine gesonderte Identitätsprüfung erforderlich ist (siehe Kapitel 3.2.3).

Die **RfA-Issuing-CA** ist in das Active Directory **der RfA** integriert. Die Identifikation/Authentifikation des Antragstellers bei der Beantragung von Zertifikaten erfolgt grundsätzlich durch eine Anmeldung mit dessen Active-Directory-Kennung, die Prüfung der Antragsberechtigung auf der Grundlage von Rechten dieser Kennung bzw. deren Gruppen-Mitgliedschaften. Die in die Zertifikate aufgenommenen Namensinformationen werden für viele Zertifikatstypen der bereits erfassten Konto-Information im Active Directory entnommen.

Daher wird die Funktion der RA größtenteils durch die Benutzer- und Rechteverwaltung **der RfA** im Active Directory erbracht.

Für folgende Zertifikatstypen, deren Namensinformation vom Antragsteller übermittelt wird, erfolgt zusätzlich vor der Zertifikatserstellung eine manuelle Prüfung durch einen Certificate Manager der **RfA-Issuing-CA**, der damit eine ergänzende RA-Funktion erbringt:

- TLS-Serverzertifikate unterschiedlicher Ausprägungen

Die RA-Funktion für TLS-Serverzertifikate der Low-Level-Management-Schnittstellen von Serversystememen (iDRAC) wird durch die Betriebsgruppe für Server-Hardware erbracht, die RA-Funktion für TLS-Serverzertifikate für verwaltete Docker-Container durch das Container-Management-System (Kubernetes) (vgl. Kapitel 3.2.5).

1.3.3 Zertifikatsnehmer

Zertifikatsnehmer der **RfA Issuing-CA** sind natürliche Personen, Funktionsaccounts und technische Systeme (Maschinen, Server und Netzwerkkomponenten) innerhalb der **RfA**. Die **RfA Issuing-CA** stellt keine weiteren CA-Zertifikate aus.

Die Zuweisung von Zertifikaten an Funktionsaccounts ist auf die folgenden Anwendungsfälle beschränkt:

- Zertifikate für technische Rollen oder zwischen Personen übertragbare Rollen innerhalb spezieller Anwendungen, namentlich für
    - Code-Signatur-Ersteller
    - Recovery-Agenten
    - Komponenten der PKI selbst, die unter Funktionsaccounts betrieben werden

1.3.4 Zertifikatsnutzer

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

1.3.5 Andere Teilnehmer

Der Betreiber der **RfA Issuing-CA** entsendet keinen Vertreter in die CA-Steuerungsgruppe.

Die Ansprechpartner der **RFA Issuing-CA** sind identisch mit denen der **RfA-CA**.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

Die **RfA Issuing-CA** stellt nur Endanwenderzertifikate für natürliche Personen, Funktionsaccounts und technische Systeme (Maschinen, Server und Netzwerkkomponenten) aus. Die erlaubte Verwendung des ausgestellten Zertifikats wird mittels der Zertifikatserweiterung KeyUsage und optional ExtendedKeyUsage gekennzeichnet.

1.4.2 Verbotene Verwendungen von Zertifikaten

Die **RfA Issuing-CA** stellt keine weiteren Sub-CA Zertifikate aus und nutzt ihren Schlüssel nicht zu Verschlüsselungs- oder Authentisierungszwecken oder für andere Signaturen als zur Zertifikats- oder Sperrlistenausstellung.

1.5 Pflege des Policy-Dokuments

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

1.5.1 Zuständigkeit für das Dokument

Die zuständigen Personen für dieses Dokument sind identisch mit dem Betreiber der **RfA Issuing-CA** (siehe Anhang 10.1).

1.5.2 Ansprechpartner/Kontaktperson/Sekretariat

Die Kontaktpersonen für dieses Policy-Dokument sind die Betreiber der **RfA Issuing-CA** (siehe Anhang 10.1).

1.5.3 Pflege dieses Dokuments

Dieses Dokument wird einmal im Jahr von dem Betreiber der **RfA Issuing-CA** (siehe Anhang 10.1) auf Aktualität und Erhalt der Konformität zur jeweils aktuellen Fassung der Anforderungen der CP Offline **RfA**-CA und der Mindestanforderungen der Rundfunk-Root-CA geprüft.

1.5.4 Annahmeverfahren für Teilnehmer-CP oder -CPS

Die **RfA Issuing-CA** hat dem Betreiber der **RfA**-CA ein CPS-Dokument vorgelegt, in dem der Zertifizierungsbetrieb und die Umsetzung der Anforderungen der Zertifizierungsrichtlinie der **RfA**-CA beschrieben sind, und erklärt, dass sie die Anforderungen der **RfA**-CA vollständig einhält und nicht abschwächt. Das Annahmeverfahren für dieses CPS-Dokument richtet sich nach den Vorgaben der Zertifizierungsrichtlinie der **RfA**-CA für Sub-CAs.

Da die **RfA Issuing-CA** ihrerseits ausschließlich Endzertifikate, aber keine CA-Zertifikate ausstellt, wird kein weiteres Annahmeverfahren für Teilnehmer-CP oder -CPS durch die **RfA Issuing-CA** benötigt.

1.5.5 Zuständiger für die Anerkennung einer CP oder eines CPS

Siehe 1.5.4

1.6 Begriffe und Abkürzungen

ACME	**Automatic Certificate Management Environment** Zertifikats-Management-Protokoll
AD	**Active Directory** Microsoft Verzeichnisdienst
Backup	Sicherung des Schlüssels bzw. einer Komponente, die auch den Schlüssel beinhaltet, mit üblichen Backup-Mechanismen, die nicht speziell für Schlüssel bestimmt sind. Z. B. also das Backup einer VM
CA	**Certification Authority** Zertifizierungsstelle
CMC	**Certificate Management using Cryptographic Message Syntax** Zertifikats-Management-Protokoll
CMP	**Certificate Management Protocol** Zertifikats-Management-Protokoll
CP	**Certificate Policy** Zertifizierungsrichtlinie
CPS	**Certification Practice Statement** Regelungen für den Zertifizierungsbetrieb
CSP	**Certificate Service Provider** Zertifizierungsdiensteanbieter
CSR	**CertificateSigningRequest** Zertifikatsantrag

CVSS	**Common Vulnerability Scoring System** Generische Methodik zur Bewertung von Schwachstellen in IT-Produkten
DCOM/RPC	**Distributed Component Object Model / Remote Procedure Call** Microsoft Netzwerkprotokoll zum Zugriff auf Windows-Dienste zur Nutzung von DCOM/RPC bei der Zertifikatsbeantragung siehe https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-WCCE/[MS-WCCE].pdf
DN	**Distinguished Name Vollqualifizierter Name** Vollqualifizierter Name
DNS	**Domain Name System** Namensauflösung im Internet
DSGVO	**Datenschutz-Grundverordnung** Verordnung (EU) Nr. 679/2016 des Europäischen Parlaments und Rates vom 27.4.2016
eIDAS	**Verordnung über elektronische Identifizierung und Vertrauensdienste** Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und Rates vom 23.07.2014
EST	**Enrollment over Secure Transport** Zertifikats-Management-Protokoll
Hinterlegung	Sichere Aufbewahrung des Schlüssels (offline und/oder verschlüsselt) für ein möglihes 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.
HTTP	**Hypertext Transfer Protocol** Hypertext-Übertragungsprotokoll

HTTPS	**Hypertext Transfer Protocol Secure** Sicheres Hypertext-Übertragungsprotokoll
IP	**Internet Protocol**
LDAP	**Lightweight Directory Access Protokoll** Protokoll zum Zugriff auf Verzeichnisdienste
MDM	**Mobile Device Management** Verwaltungssystem für Mobilgeräte
OCSP	**Online Certificate Status Protocol** Online-Auskunftsdienst zum Status von Zertifikaten
OID	**Object Identifier** Eindeutiger Kennzeichner für Objekte
PKI	**Public Key Infrastructure** Infrastruktur für X.509 Zertifikate
RA	**Registration Authority** Registrierungsstelle
REST	Representational State Transfer Verfahren für den Zugriff auf Web-Services
SCEP	**Simple Certificate Management Protocol** Zertifikats-Management-Protokoll
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.
SID	**Security Identifier** Eindeutiger Identifier eines Benutzers oder Computers im Active Directory
SIEM	**Security Information and Event Management** System zur Erkennung und Behandlung von Sicherheitsvorfällen
SOAP	ursprünglich für **Simple Object Access Protocol** Netzwerkprotokoll für den Zugriff auf Web-Services
Speicherung	Ablage des Schlüssels zum bestimmungsgemäßen Gebrauch durch den Schlüsselinhaber, ggf. auch in persistentem Speicher, sprich auf Disk, oder in einem HSM
SPN	**Service Principal Name** Eindeutiges Benamungsschema von Computerobjekten und -anwendungen im Active Directory
TLS	**Transport Layer Security** Netzwerksicherheitsprotokoll für vertrauliche und integritätsgeschützte Verbindungen
UPN	**User Principal Name** Eindeutiges Benamungs-Schema von Benutzerobjekten im Active Directory
Wiederherstellung	Erneute Speicherung des Schlüssels aus Hinterlegung, Sicherung oder Backup.

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Die **RfA Issuing-CA** stellt ihre Verifikationsinformationen (CA-Zertifikat und Sperrinformationen) für die Zertifikatsnutzer der von ihr erstellten Zertifikate über Web-basierte PKI-

Veröffentlichungspunkte unter den u. a. URLs bereit. Die Zertifikatsnutzer können interne und/oder externe Nutzer (Personen, Systeme und Organisationen) sowie Nutzer im ARD-Netz sein.

- RfA-intern : http://ca-info.br-edv.brnet.int/Zert-Infos/
- ARD-Netz: http://ca-info.br.cn.ard.de/Zert-Infos/
- Internet: http://ca-info.br.de/Zert-Infos/

Bei der Veröffentlichung stellt sie sicher, dass eine mögliche Veröffentlichung personenbezogener Daten nicht den geltenden Datenschutzrichtlinien widerspricht. Dazu verwendete Webserver werden entsprechend dem Stand der Technik und nach den geltenden Sicherheitsrichtlinien der **RfA** betrieben.

Zusätzlich stellt die **RfA Issuing-CA** internen Zertifikatsnutzern ihr eigenes CA-Zertifikat und Sperrinformationen zu den von ihr ausgestellten Zertifikaten per LDAP im Active Directory (AD) der **RfA** zur Verfügung. Diese Daten enthalten keine direkt personenbeziehbaren Daten.

Auch das AD wird entsprechend dem Stand der Technik und nach den geltenden Sicherheitsrichtlinien der **RfA** betrieben.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

Die **RFA Issuing-CA** stellt auf den in Kapitel 2.1 genannten PKI-Veröffentlichungspunkten die folgenden Informationen zur Verfügung:

- dieses CPS-Dokument
- das Zertifikat der **RFA Issuing-CA** und dessen Fingerabdruck
- die CRL der **RFA Issuing-CA**
- die Kontaktinformationen, unter denen die Sperrung eines Teilnehmerzertifikats beantragt werden kann

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

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Die Veröffentlichung von Sperrinformationen nach durchgeführter Sperrung eines von der **RfA Issuing-CA** ausgestellten Zertifikats erfolgt in der Regel unverzüglich, spätestens jedoch nach 24 Stunden automatisch.

2.4 Zugriffskontrollen auf Verzeichnisse

Unkontrollierte Änderungen von Zertifikaten und Sperrinformationen im AD sowie auf den Web-basierten PKI-Veröffentlichungspunkten für den Zugriff aus dem **RfA** internen LAN, im ARD-Netz und im Internet werden durch entsprechende Berechtigungskonzepte verhindert. Der lesende Zugriff auf die Informationen ist ohne vorherige Anmeldung möglich. Der schreibende Zugriff ist auf die Gruppe der PKI-Administratoren und deren Vertreter, technische Accounts, die für die automatisierte Veröffentlichung genutzt werden, sowie die Administratoren der jeweils genutzten Webserver bzw. Verzeichnisdienste beschränkt.

Zertifikate und Sperrlisten sind durch eine digitale Signatur der ausstellende CA gegen Manipulation geschützt. Somit kann jederzeit von jedem Zertifikatsnutzer geprüft werden, ob die Integrität der Zertifikate und Sperrlisten gewährleistet ist und ob sie von einem vertrauenswürdigen Herausgeber stammen.

3. Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

Die Namensgebung in Zertifikaten entspricht dem X.500 Standard. Weitere Namensformen sind darüber hinaus möglich.

Insbesondere kann die **RfA-Issuing-CA** nach Bedarf der Zertifikats-nutzenden Anwendungen eine oder mehrere der folgenden Arten von Namensinformationen in die Zertifikate aufnehmen:

- E-Mail-Adresse
- DNS-Name
- IP-Adresse
- Universal Principal Name (UPN) oder Service Principal Name (SPN) im Active Directory
- Security Identifier (SID) im Active Directory

3.1.2 Notwendigkeit für aussagefähige Namen

Der Inhabername im CA-Zertifikat der **RfA Issuing-CA** wurde gemäß den Regelungen der ausstellenden CA festgelegt und ist entsprechend aussagekräftig.

In den von ihr ausgestellten Endanwenderzertifikaten verwendet die **RfA Issuing-CA** im Kontext der jeweiligen PKI-Anwendung aussagekräftige Inhaber-Namen, um die Identität des Endnutzers oder -systems klar erkenntlich zu machen.

Im subject Name eines RfA Zertifikates (Sub-CA bzw. Endanwenderzertifikat) ist mindestens eine CN-Komponente enthalten. Die CN-, O- und C-Komponenten der **RfA Issuing-CA** lauten: CN=BR-SubCA-2032, O=Bayerischer Rundfunk, C=DE.

Die Identität des Endnutzers oder -systems wird nicht verschleiert oder verborgen, muss aber ggf. im Kontext der jeweiligen PKI-Anwendung und deren IT-Infrastrukturkomponenten interpretiert werden. Beispielsweise kann, um die Identität eines Gerätes am Zertifikatsnamen erkennen zu können, auch die Seriennummer des Gerätes oder die Identität des Besitzers, dem das Gerät im betreffenden Management-System fest zugeordnet ist, als Zertifikatsname genutzt werden.

Falls IP-Adressen als Namensformen in Zertifikate aufgenommen werden, müssen diese dem betreffenden System der **RfA** im internen LAN oder im ARD-Netz (CN) zugewiesen sein.

3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern

Es werden keine Pseudonyme verwendet. Die Zertifikate können eindeutig den Zertifikatsinhabern zugeordnet werden.

Identifier, die über ein Managementsystem (bspw. das AD oder ein MDM) verwaltet werden, fallen nicht unter Pseudonyme, selbst wenn sie nur unter Rückgriff auf - ggf. zugriffsbeschränkte - Informationen des betreffenden Managementsystems zugeordnet werden können.

Ein Wildcard-Zertifikat wird nur in Ausnahmefällen für eine dem Verwendungszweck entsprechende Subdomain (z.B. *.ad.rfa.de) ausgestellt. Des Weiteren wird der Verwendungszweck/Begründung, Ausstellungsdatum und Ablaufdatum in Kapitel 10.2.1 dokumentiert.

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Die Distinguished Names im "subject" und "issuer" Feld des Zertifikats bezeichnen eindeutig den Zertifikatsinhaber und -herausgeber. Alternativ kann der Zertifikatsinhaber auch in der SubjectAltName Erweiterung benannt werden. Diese SubjectAltName Erweiterung kann weitere Namensformen für den Zertifikatsinhaber enthalten, die im Kontext der PKI-Anwendung, für die das Zertifikat genutzt wird, interpretierbar sind, wie bspw. E-Mail Adresse, UPN, DNS-Name oder IP-Adresse (vgl. 3.1.1).

In ausgestellten Zertifikaten mit leerem "subject" Feld ist stets eine als kritisch markierte SubjectAltName Erweiterung mit mindestens einem Namenseintrag enthalten.

Die mindestens enthaltene Namensinformation ist für die unterschiedlichen unterstützten Zertifikatstypen nach den Erfordernissen der jeweiligen PKI-nutzenden Anwendung(en) festgelegt, die diese Namensformen interpretieren müssen, siehe Abschnitt 7.1.4.

3.1.5 Eindeutigkeit von Namen

Bei der Vergabe von Namen wird sichergestellt, dass der Name des Zertifikatsinhabers innerhalb der ausstellenden CA eindeutig ist.

- Bei manueller Vergabe: Der zuständige Certificate Manager prüft vor der Ausstellung, ob (Host/Anwendungs/Alias)-Name bereits im DNS und/oder AD existiert. Stichprobenartig wird auch unter den „Issued Certificates“ geprüft, ob ein „Issued Common Name“ bereits existiert.
- Bei automatischer Vergabe: Das System liest den aus dem führenden Verzeichnis oder der Datenbank des führenden Management-Systems aus. Somit ist eine Eindeutigkeit gegeben.

3.1.6 Anerkennung, Authentifizierung und Rolle von Markennamen

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

3.2 Erstmalige Überprüfung der Identität

3.2.1 Methoden zur Überprüfung des Besitzes des privaten Schlüssels

Um sicherzustellen, dass der Antragsteller im Besitz des zugehörigen privaten Schlüssels ist, muss der Zertifikatsantrag (CSR) an die **RFA Issuing-CA** mit dem privaten Schlüssel des Antragstellers digital signiert sein. Die **RFA Issuing-CA** akzeptiert nur digital signierte Zertifikatsanträge und prüft diese Signatur auf Gültigkeit und Korrektheit.

3.2.2 Authentifizierung von Organisationszugehörigkeiten

Beim Zertifikatsantrag durch einen Endanwender muss keine Organisationszugehörigkeit überprüft werden.

Im Regelfall werden Zertifikate für Angehörige oder Systeme der **RfA** vergeben. In diesem Fall kann die **RfA Issuing-CA** die entsprechende Organisationszugehörigkeit im ausgestellten Zertifikat eigenständig ergänzen.

3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikatsnehmers

Die Authentifizierung des Antragstellers erfolgt auf Basis bereits erfasster Daten, persönlicher Bekanntschaft des Antragstellers bei den PKI Administratoren (Certificate Manager s. o.) oder durch Rückfragen bei Kollegen bzw. Vorgesetzten. Nur wenn das nicht möglich ist, wird beim Neuantrag auf Zertifizierung eine gesonderte Identitätsprüfung des Antragstellers durch den Certificate Manager der CA durchgeführt.

Sofern der Antragsteller für einen Dritten handelt (z.B. SCEP-Proxy), hat der Antragsteller die Authentifizierung des Dritten wie oben beschrieben vorzunehmen.

Die Identitätsprüfung und Authentifikation des Antragstellers bei der **RfA Issuing-CA** erfolgt durch eine Anmeldung mit den AD-Credentials (Benutzername und Passwort oder gültiges Kerberos-Ticket) des Antragstellers, wenn die Zertifikatsbeantragung über eine der folgenden Schnittstellen erfolgt:

- Native Schnittstelle der AD Certificate Services (Microsoft DCOM/RPC)
- Web-Enrollment-Schnittstelle (Microsoft CA Web Enrollment)
- REST-Schnittstelle (AdcsToRest)

3.2.4 Ungeprüfte Zertifikatsnehmerangaben

Die **RFA Issuing-CA** nimmt keine ungeprüften Teilnehmerangaben in die Endanwenderzertifikaten auf.

Bei automatisiert ausgestellten Zertifikaten (Auto Enrollment) ohne Prüfung des Zertifikatsantrags durch einen Certificate Manager wird durch technische Sicherheitsmechanismen und Berechtigungseinstellungen der jeweils verwendeten IT-Infrastrukturkomponenten und/oder Antragsprotokolle (bspw. Windows Auto-Enrollment im AD) entsprechend dem Stand der Technik verhindert, dass der Antragsteller einen Zertifikatsantrag mit unberechtigten Angaben erstellt oder manuell verändert.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Die **RFA Issuing-CA** stellt Zertifikate nur nach Prüfung der Berechtigung des Antragstellers aus. Hierbei kann die Berechtigungsprüfung eines Antragstellers automatisch und auch schon vorab erfolgen, so dass nur berechtigte Nutzer überhaupt einen Zertifikatsantrag stellen können. Folgende alternative Prozesse zur Prüfung der Berechtigung zur Antragsstellung finden Anwendung:

- Die Berechtigung zur Zertifikatsbeantragung wird über AD-Gruppen kontrolliert. AD-Administratoren nehmen in Übereinstimmung mit den Regelungen der **RfA** zur Benutzerverwaltung AD-Benutzer und/oder -Computer in die jeweiligen Rechtegruppen für die Beantragung bestimmter Zertifikatstypen auf.

- Für Benutzer und/oder Systeme eines eindeutig definierten Anwendungsbereichs innerhalb der **RfA** kann die **RfA Issuing-CA** die Vergabe und Prüfung der Berechtigung zur Antragstellung für die jeweils benötigten Zertifikate an die zuständige Fachgruppe oder an das betreffende Management-System delegieren, die bzw. das die Benutzer und/oder Systeme in diesem Anwendungsbereich verwaltet. Von dieser Möglichkeit wird in den folgenden Anwendungsbereichen Gebrauch gemacht:
    - An die Betriebsgruppe für Server-Hardware für Serverzertifikate der Low-Level-Management-Schnittstellen der verwalteten Serversysteme (Dell iDRAC, HP iLO oder IPMI-Schnittstellen anderer Hersteller)
    - An das Container-Management-System (Kubernetes) für Serverzertifikate für die darüber verwalteten Docker-Container
    - An die Betriebsgruppe des Microsoft System Center Operations Manager (SCOM) für Serverzertifikate für die SCOM-Server und -Dienst
    - An die Verantwortlichen für die interne Softwareentwicklung für Code-Signatur-Zertifikate
- CA-Administratoren der **RfA Issuing-CA** können in begründeten Fällen einzelne Benutzer oder Systeme zur Antragstellung berechtigen. Die Plausibilität der Begründung wird durch die CA-Administratoren nach eigenem Ermessen geprüft.

3.2.6 Kriterien zur Zusammenarbeit

Für eine Zertifikatsinfrastruktur-übergreifende Zusammenarbeit müssen andere Zertifikatsinfrastrukturen die Mindestanforderungen der Rundfunk-Root-CA erfüllen. Es besteht keine weitere Zusammenarbeit mit PKIs außerhalb der Rundfunkanstalten.

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 die (Über-)Signatur des neuen Zertifikatsantrags mit dem noch gültigen Zertifikat herangezogen wird. In diesem Fall werden die Angaben zum Zertifikatsinhaber unverändert aus dem bestehenden Zertifikat übernommen.

Diese Möglichkeit kann von der **RfA-Issuing-CA** für bestimmte Zertifikatstypen angeboten werden, wo dies in den Antragsprotokollen (bspw. Microsoft Certificate Enrollment oder SCEP) technisch unterstützt wird und zur Automatisierung des Zertifikats-Erneuerungsprozesses sinnvoll ist.

Ist das Zertifikat jedoch schon abgelaufen oder wird diese Möglichkeit vom Antragsteller nicht genutzt, 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 ein Zertifikat 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

Bei einem Sperrantrag für ein Endanwenderzertifikat ist keine gesonderte Identitätsprüfung durch die ausstellende CA erforderlich, wenn der Antragsteller dem Betreiber der **RFA Issuing-CA** persönlich bekannt ist. Ansonsten führt ein Certificate Manager eine geeignete Identitätsprüfung des Antragstellers durch, die sich nach der Form des Sperrantrags richtet:

- Prüfung eines Lichtbild-Ausweises 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
- Sichtung der Identität des Ticket-Initiators bei Sperranträgen über das Helpdesk-System

Bevor ein CA-Administrator jedoch ein Endteilnehmerzertifikat in der BR-SubCA-2023 sperrt, muss sich ein Mitarbeiter der Fachgruppe Rechenzentren und IT-Systeme über die Sperrabsicht vergewissern:

- Ein TLS-Serverzertifikat wird nur nach Rücksprache mit dem Inhaber des Servers/Systems gesperrt.
- Ein Benutzerzertifikat wird nur nach Rücksprache mit dem Benutzer oder seinem direktenVorgesetzten gesperrt.
- Ein WLAN-Zertifikat wird nur nach Rücksprache mit einem Client-Administrator gesperrt.

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).

Zu den Prozessen für die Vergabe von Berechtigungen zur Antragstellung siehe Abschnitt 3.2.5.

4.1.2 Registrierungsprozess und Zuständigkeiten

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

Zertifikate können entweder manuell oder automatisch beantragt werden. Sie sollen nach Möglichkeit automatisiert beantragt werden. Dazu werden technische Schnittstellen angeboten, über die eine automatische Zertifikatsbeantragung unterstützt wird.

Zertifikatsanträge, bei denen der Name des Zertifikatsinhabers vom Antragsteller frei gewählt werden kann, erfordern grundsätzlich eine Prüfung und Freigabe des Zertifikatsantrags durch einen Certificate Manager, bevor das Zertifikat ausgestellt werden darf.

In den Fällen, in denen die Vergabe und Prüfung der Berechtigung zur Zertifikatsbeantragung an Betriebsverantwortliche oder an ein Management-System delegiert wurde (siehe Abschnitt 3.2.5) obliegt die Prüfung von frei wählbaren Antragstellernamen dem Betriebsverantwortlichen bzw. Management-System (vgl. Abschnitt 4.2.2).

In diesen Fällen darf auch der Betriebsverantwortliche bzw. das Management-System stellvertretend für den Zertifikatsinhaber ein Schlüsselpaar erzeugen und den öffentlichen Schlüssel gesichert in einem Zertifikatsantrag (CSR) bei der CA einreichen. Falls von dieser Möglichkeit Gebrauch gemacht wird, werden zur Übermittlung des privaten Schlüssels an den Zertifikatsinhaber entweder die vorhandenen Sicherheitsmechanismen des jeweiligen Management-Systems zur gesicherten Kommunikation mit den verwalteten Systemen genutzt. Oder die Weitergabe erfolgt manuell durch einen Betriebsverantwortlichen, bspw. durch persönlichen Kontakt. Die Betriebsverantwortlichen der Anwendungsbereiche, für die Vergabe und Prüfung der Berechtigung zur Zertifikatsbeantragung delegiert wurde, sichern der **RfA Issuing-CA** zu, dass die Art der Übermittlung des privaten Schlüssels den Sicherheitsanforderungen in ihrem Anwendungsbereich und den diesbezüglichen internen Regelungen der **RfA** genügt.

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Bei einer Zertifikatsbeantragung ist keine gesonderte Identitätsprüfung erforderlich, wenn die Identitätsfeststellung durch die Anmeldung an der CA bei der Zertifikatsbeantragung gesichert ist. Ansonsten wird beim Neuantrag auf Zertifizierung eine gesonderte Identitätsprüfung des Antragstellers durchgeführt und als Ticket im Helpdesk-System dokumentiert.

Die zur Identitätsprüfung und Authentifizierung bei der Zertifikatsbeantragung genutzten Verfahren sind in Abschnitt 3.2.3 dokumentiert.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Die **RFA Issuing-CA** bietet die folgenden technischen Schnittstellen zur Zertifikatsbeantragung an:

- Microsoft Windows Client Certificate Enrollment per DCOM/RPC
- Web-Schnittstelle (Microsoft CA Web Enrollment)
- REST-Web-Service (AdcsToRest)

Zertifikatsanträge, bei denen der Name des Zertifikatsinhabers vom Antragsteller frei gewählt werden kann, erfordern eine Prüfung und Freigabe des Zertifikatsantrags durch einen Certificate Manager, bevor das Zertifikat ausgestellt wird (siehe auch Abschnitt 4.1.2).

Folgende Felder werden bei der manuellen Prüfung eines Antrags für ein TLS-Zertifikats (z.B. für Webserver) durch einen Certificate Manager einbezogen:

- CN (Common Name) *: Hostname, FQDN oder Applikationsbezeichnung

- E-Mail **: Kontakt-E-Mail-Adresse innerhalb der **RFA**
- OU (Organizational Unit) **: Betreibende Einheit innerhalb der **RFA**
- O (Organization) **: Name der **RFA**
- C (Country) **: DE
- SAN (Subject Alternative Name) * : DNS-Hostnamen und optional IP-Adressen des Servers, unter denen dieser im LAN oder ggf. im ARD-Netz registriert und erreichbar ist

* = Pflichtfeld** = optionales Feld

Sind die Pflichtangaben nicht vorhanden oder fehlerhaft, die optionalen Felder enthalten aber fehlerhaft oder weitere Namensfelder vorhanden wird die Ausstellung des Zertifikates abgelehnt. Der Antragsteller wird über die Ablehnung seines Antrages benachrichtigt.

Als zusätzliche Sicherheitsmaßnahme werden Anträge für Zertifikatstypen, bei denen der Name vom Antragsteller gewählt werden darf und bei denen die Registrierung delegiert ist, automatisiert gegen eine schwarze Liste (Blacklist) von Namen besonders berechtigter Konten (z. B. AD-Administratoren, AD-Domain-Controller) geprüft. Ist einer der Namen auf der Blacklist im Zertifikatsantrag enthalten, wird die Ausstellung des Zertifikats abgelehnt.

Die Blacklist wird von den AD-Administratoren gepflegt.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Die Bearbeitungsdauer für Zertifikatsanträge ist nicht festgelegt. Es erfolgt eine zeitnahe Bearbeitung.

4.3 Zertifikatsausgabe

4.3.1 Aktionen des Zertifizierungsdiensteanbieters bei der Ausgabe von Zertifikaten

Eine Erstellung von Zertifikaten erfolgt nur für gültige Zertifikatsanträge, die syntaktisch korrekt sind und alle für den jeweiligen Zertifikatstyp erforderlichen Informationen im Antrag enthalten (vgl. Abschnitt 4.2.2 und 7.1), so dass auf dieser Basis ein Zertifikat erstellt wurde.

Die Übermittlung des ausgestellten Zertifikates erfolgt grundsätzlich über die beim Zertifikatsantrag genutzte technische Schnittstelle zur Zertifikatsbeantragung (vgl. Abschnitt 4.2.2) oder ausnahmsweise manuell durch einen Certificate Manager.

Die Verbindung zwischen Zertifikatsinhaber und dem zugehörigen Schlüsselpaar ist durch die Überprüfung nach Abschnitt 3.2.1 sichergestellt.

In den Fällen, in denen die Vergabe und Prüfung der Berechtigung zur Zertifikatsbeantragung an Betriebsverantwortliche oder an ein Management-System delegiert wurde (siehe Abschnitt 3.2.5) und dieser bzw. dieses stellvertretend für den Zertifikatsinhaber das Zertifikat beantragt, wird das Zertifikat an den beantragenden Betriebsverantwortlichen bzw. das Management-System übermittelt. Es obliegt diesem, das Zertifikat sowie ggf. einen stellvertretend generierten privaten Schlüssel an den Zertifikatsinhaber weiter zu leiten, siehe auch Abschnitt 4.1.2.

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

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

4.4 Zertifikatsannahme

4.4.1 Verhalten für eine Zertifikatsannahme

Der Zertifikatnehmer ist verpflichtet, die Korrektheit des eigenen Zertifikats sowie des Zertifikats der ausstellenden CA nach Erhalt zu verifizieren. Diese Prüfung kann auch automatisiert und ohne Dokumentation erfolgen.

4.4.2 Veröffentlichung des Zertifikats durch die CA

Die **RFA Issuing-CA** veröffentlicht ihr CA-Zertifikat so, dass dieses ARD-Netz-weit abgerufen werden kann (siehe Kap. 1.3.4).

Sollten zukünftig von der **RFA Issuing-CA** Verschlüsselungszertifikate für Benutzer ausgegeben werden, die auch von anderen Rundfunkanstalten genutzt werden sollen, so werden diese ebenfalls im ARD-Netz veröffentlicht. Dies ist derzeit nicht der Fall.

4.4.3 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe des Zertifikats

Eine Benachrichtigung weiterer Zertifikatsinfrastruktur-Teilnehmer ist nicht vorgesehen.

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 die **RFA Issuing-CA** selbst als auch für die von dieser zertifizierten Endanwender:

- Ein Zertifikatsnehmer (engl.: Subscribing Party) darf seinen Schlüssel und Zertifikat nur für die im Zertifikat genannten Verwendungszwecke und unter Einhaltung der weiteren Anforderungen in diesem Dokument sowie den Policy-Dokumenten der darüberliegenden CAs einsetzen.
- Ein Zertifikatsnehmer muss Sorge tragen, dass sein privater Schlüssel angemessen vor Diebstahl, Missbrauch und Verlust geschützt ist. Dies gilt auch für Backups der Schlüssel.
- Ein Zertifikat ist unverzüglich zu sperren, wenn die Angaben des Zertifikats nicht mehr korrekt sind oder wenn der private Schlüssel abhandengekommen ist, gestohlen oder möglicherweise kompromittiert wurde.
- Die **RFA Issuing-CA** bietet keine Möglichkeit der Schlüsselhinterlegung an. Daher ist der Zertifikatsnehmer selbst dazu verpflichtet, private Schlüssel so zu sichern, dass er ggf. verschlüsselte Daten wieder entschlüsseln kann.
- Die **RFA Issuing-CA** bietet eine Schlüsselhinterlegung für S/MIME-Verschlüsselungszertifikate an (siehe Abschnitt 4.12). Falls diese Möglichkeit nicht genutzt wird sowie für alle anderen

Zertifikatstypen ist der Zertifikatsnehmer selbst dazu verpflichtet, private Schlüssel so zu sichern, dass er ggf. verschlüsselte Daten wieder entschlüsseln kann.

Wie die **RFA Issuing-CA** dafür Sorge trägt, dass sie ihre eigenen Schlüssel im Notfall wiederherstellen kann, um einen kontinuierlichen Zertifizierungsbetrieb zu gewährleisten sowie die weiteren oben genannten Anforderungen selbst einhält, ist in den Kapiteln 5 und 6 dargelegt.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Ein Zertifikatsprüfer (engl.: Relying Party) ist dazu verpflichtet, ein Zertifikat nur für die im Zertifikat (insbesondere in den KeyUsage und ExtendedKeyUsage Erweiterungen) genannten Verwendungszwecke akzeptieren.

Die **RfA Issuing-CA** kann die Einhaltung dieser Verpflichtung jedoch nicht kontrollieren. Etwaige Schäden, die sich aus der Nichteinhaltung dieser Verpflichtung ergeben, gehen zulasten des jeweiligen Zertifikatsprüfers.

4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüsselpaars (certificate renewal)

4.6.1 Bedingungen für eine Zertifikatserneuerung

Die **RFA Issuing-CA** selbst wird keine Zertifikatserneuerung unter Beibehaltung des alten Schlüsselpaars beantragen (vgl. Abschnitt 4.7.1).

Dasselbe gilt grundsätzlich 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 bei Bedarf beibehalten und nur das Zertifikat erneuert werden.

Eine Zertifikatserneuerung eines Endanwenderzertifikats unter Beibehaltung des alten Schlüsselpaars kann beantragt werden, wenn z.B. die Gültigkeit eines Zertifikats abläuft.

4.6.2 Wer darf eine Zertifikatserneuerung beantragen?

Eine Zertifikatserneuerung wird grundsätzlich durch den Zertifikatsnehmer bzw. eine autorisierte Person [5] beantragt. Die **RFA Issuing-CA** kann im eigenen Ermessen eine Zertifikatserneuerung von Endanwenderzertifikaten aktiv unterstützen - bspw. durch Versenden von Erinnerungs-E-Mails - um den Prozess der Zertifikatserneuerung zu verbessern.

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

4.6.3 Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung

Die Bearbeitung eines Antrags auf Zertifikatserneuerung wird grundsätzlich wie bei der erstmaligen Zertifikatsbeantragung durchgeführt (siehe Kap. 4.1 und 4.2).

Alternativ und optional kann der Antragsteller bei der Beantragung einer Zertifikatserneuerung den Zertifikats-Request mit zu dem erneuernden Zertifikat und dem zugehörigen privaten Schlüssel signieren. Wenn die Namensinformation des erneuerten Zertifikats identisch zu dem vorherigen,

bereits geprüften Zertifikat übernommen wird, entfällt dabei eine im Erstantrag ggf. notwendige manuell Prüfung durch einen Certificate Manager. Diese Art der Zertifikatserneuerung wird bei folgenden technischen Schnittstellen (vgl. Kap. 4.2.2) angeboten:

- Microsoft Windows Client Certificate Enrollment
- REST-Web-Service

4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Es muss keine zusätzliche Benachrichtigung bzgl. der Zertifikatserstellung stattfinden.

4.6.5 Verhalten für die Annahme einer Zertifikatserneuerung

Es gelten die Regelungen gemäß Abschnitt 4.4.1

4.6.6 Veröffentlichung der Zertifikatserneuerung durch die CA

Es gelten die Regelungen gemäß Abschnitt 4.4.2.

4.6.7 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Erneuerung des Zertifikats

Eine Benachrichtigung ist nicht vorgesehen.

4.7 Zertifikatserneuerung mit Schlüsselerneuerung

4.7.1 Bedingungen für eine Zertifizierung nach Schlüsselerneuerung

Die **RFA Issuing-CA** selbst wird eine Zertifikatserneuerung mit Schlüsselerneuerung beantragen, wenn die Gültigkeit ihres Zertifikats abläuft und das CA-Zertifikat noch benötigt wird.

Eine Zertifikatserneuerung 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 aber weiterhin ein Zertifikat benötigt wird.

Auch Endanwender als Zertifikatsinhaber sind hierzu verpflichtet.

4.7.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen?

Es gelten die Regelungen wie bei einer Zertifikatserneuerung (Abschnitt 4.6.2).

4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Es gelten die Regelungen wie bei einer Zertifikatserneuerung (Abschnitt 4.6.3).

4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Es muss keine zusätzliche Benachrichtigung bzgl. der Zertifikatserstellung stattfinden.

4.7.5 Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen

Es gelten die Regelungen wie bei einer Zertifikatserneuerung (Abschnitt 4.6.5).

4.7.6 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA

Es gelten die Regelungen gemäß Abschnitt 4.4.2.

4.7.7 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Eine Benachrichtigung ist nicht vorgesehen.

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,
- der Name des Systems stimmt nicht mehr mit dem Namen im CN-Feld des Zertifikates überein,
- die Zuordnung der im Zertifikat enthaltenen E-Mail-Adresse zum Zertifikatsnehmer ist nicht mehr gegeben.

4.8.2 Wer darf eine Zertifikatsänderung beantragen?

Es gelten die Regelungen wie bei einer erstmaligen Zertifikatsbeantragung (Kapitel 4.1.1).

4.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung

Es gelten die Regelungen wie bei einer erstmaligen Zertifikatsbeantragung (Kapitel 4.2).

4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Es muss keine zusätzliche Benachrichtigung bzgl. der Zertifikatserstellung stattfinden.

4.8.5 Verhalten für die Annahme einer Zertifikatsänderung

Es gelten die Regelungen wie bei einer Zertifikatserneuerung (Abschnitt 4.6.5).

4.8.6 Veröffentlichung der Zertifikatsänderung durch die CA

Es gelten die Regelungen gemäß Abschnitt 4.4.2.

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

Eine Benachrichtigung ist nicht vorgesehen.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Bedingungen für eine Sperrung

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

- Das Zertifikat enthält Angaben, die nicht gültig sind.

- Der private Schlüssel des Zertifikatsnehmers wurde verloren, gestohlen, offengelegt oder anderweitig kompromittiert bzw. missbraucht.
- Der Zertifikatsnehmer ist nicht mehr berechtigt, das Zertifikat zu nutzen.
- Der Zertifikatsnehmer hält seine Verpflichtungen aus dem relevanten CP bzw. diesem CPS nicht ein, insbesondere die Verpflichtungen zum Umgang mit dem Zertifikat und dem privaten Schlüssel.
- Die zuständige **RfA Issuing-CA** hält die CP oder das CPS nicht ein.
- Die **RfA Issuing-CA** oder die **RfA-CA** stellt den Zertifizierungsbetrieb ein.
- Der Zertifikatsnehmer benötigt das Zertifikat nicht mehr.

4.9.2 Wer kann eine Sperrung beantragen?

Bei Verdacht auf Kompromittierung des **RfA Issuing-CA** Schlüssels oder bei Einstellung des Betriebs der **RfA Issuing-CA** muss einer der CA-Administratoren der **RfA Issuing-CA** einen Sperrantrag bei der **RfA-CA** stellen. Auch der zuständige IT-Sicherheitsbeauftragte darf die Sperrung des **RfA Issuing-CA** Zertifikats beantragen, wenn bspw. die Mindestanforderungen aus der CP für Issuing-CAs der **RfA-CA** durch die betreffende Issuing-CA nicht eingehalten werden.

Bei Verdacht auf Kompromittierung des privaten Schlüssels eines Endanwenders, bei Verlust des privaten Schlüssels, wenn das Zertifikat nicht mehr benötigt wird oder ein anderer der in Kapitel 4.9.1 genannten Sperrgründe vorliegt, ist der Endanwender bzw. im Fall eines Serverzertifikats der zuständige Administrator verpflichtet, einen Sperrantrag bei der **RfA Issuing-CA zu** stellen, die das Zertifikat ausgestellt hat.

Falls den Certificate Managern der **RfA Issuing-CA** durch Dritte ein Sachverhalt bekannt wird, der die Sperrung eines Zertifikats erfordert (vgl. Kapitel 4.9.1), prüfen sie diese Information auf Stichhaltigkeit und stellen ggf. selbst einen Sperrantrag.

4.9.3 Verfahren für einen Sperrantrag

Das Verfahren und die Berechtigung für die Beantragung einer Zertifikatssperrung ist von der **RfA Issuing-CA** in diesem Dokument dokumentiert und den Zertifikatsnehmern bekannt gegeben worden.

Grundsätzlich sind alle Zertifikatsarbeiten im Ticketsystem des Servicedesks der **RfA** zu dokumentieren.

1. Zertifikatsnehmer gibt einen Call beim Servicedesk der RfA für Zertifikatssperrung auf.
2. Call wird durch den Servicedesk Mitarbeiter aufgenommen und es wird ein Ticket für die Certificate Manager erstellt.
3. Weiterbearbeitung des Ticketdurch einen Certificate Manager (Prüfung, ob Antragsteller sperrberechtigt ist, Plausibilitätsprüfung des Sperrgrunds, Rückfragen nach Kap. 3.4).
4. Zertifikat wird nach erfolgreicher Prüfung gesperrt.
5. Neue Sperrliste wird umgehend erstellt und veröffentlicht.

6. Mitteilung an Antragsteller über die Sperrung des Zertifikates durch Mitteilung über das abgeschlossene Ticket durch das Ticketsystem.

Bei einem Sperrantrag für ein Endanwenderzertifikat gelten die Anforderungen zur Identitätsfeststellung, die in Kapitel 3.4 beschrieben sind.

Sperranträge können alternativ per E-Mail an das Postfach der PKI-Administration gestellt werden.

1. Zertifikatsnehmer schreibt eine E-Mail an **pki.manager@br.de**
2. Erstellung eines Tickets durch einen Certificate Manager
3. Weiterbearbeitung des Tickets durch einen Certificate Manager (Prüfung, ob Antragsteller sperrberechtigt ist, Plausibilitätsprüfung des Sperrgrunds, Rückfragen nach Kap. 3.4).
4. Zertifikat wird nach erfolgreicher Prüfung gesperrt.
5. Neue Sperrliste wird umgehend erstellt und veröffentlicht.
6. Mitteilung an Antragsteller über die Sperrung des Zertifikates durch Mitteilung über das abgeschlossene Ticket durch das Ticketsystem.

In den Fällen, in denen die Vergabe und Prüfung der Berechtigung zur Zertifikatsbeantragung an Betriebsverantwortliche oder an ein Management-System delegiert wurde (siehe Abschnitt 3.2.5) erhalten diese bei Bedarf die Berechtigung, die Zertifikate von verwalteten Geräten zu sperren, falls ein Gerät als verlustig gemeldet wird (verloren, gestohlen, defekt) oder aus anderen Gründen außer Betrieb genommen wird.

Der Prozess zur Feststellung und Dokumentation dieser Fälle richtet sich nach den Vorgaben und Regelungen für das jeweilige Management-System.

Dies wird derzeit umgesetzt für:

- noch keine Betriebsverantwortliche oder Management-Systeme

4.9.4 Fristen für einen Sperrantrag

Bei Bekanntwerden eines Sperrgrundes muss unverzüglich die Sperrung beantragt werden.

Die **RfA Issuing-CA** hat jedoch keine verlässliche Möglichkeit, die Einhaltung dieser Verpflichtung durch ihre Zertifikatnehmer zu prüfen.

4.9.5 Fristen/Zeitspanne für die Bearbeitung des Sperrantrags durch die CA

Sperranträge werden unverzüglich bearbeitet. Bei Vorliegen eines berechtigten Sperrgrunds wird das betreffende Zertifikat unverzüglich gesperrt.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Die **RFA Issuing-CA** stellt den Zertifikatsprüfern RFA-übergreifend, d. h. mindestens intern und im ARD-Netz Sperrinformationen zu ihren ausgestellten Zertifikaten zur Verfügung.

Sperrlisten (CRLs) werden in den folgenden Netzen veröffentlicht (vgl. Kapitel 2):

- Internes Netz der RfA
- ARD-Netz
- Internet

Eine Online-Statusanfrage per OCSP wird in den folgenden Netzen angeboten (vgl. Kapitel 2):

- Internes Netz der RfA

4.9.7 Frequenz der Veröffentlichung von Sperrlisten

Die Sperrliste der **RFA Issuing-CA** ist zwei Tage gültig. Alle 24 Stunden wird eine neue Sperrliste erstellt. Im Falle einer Sperrung eines Zertifikats wird zusätzlich eine neue Sperrliste ausgestellt und veröffentlicht werden die ebenfalls wieder zwei Tage gültig ist.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die Sperrlisten sind maximal 24 Stunden länger gültig als der Ausstellungszyklus der Sperrliste.

4.9.9 Verfügbarkeit von Online-Sperrinformationen

Die **RFA Issuing-CA** bietet einen OCSP-Dienst an. Der OCSP-Dienst wird wie folgt in die Zertifikate eingetragen.

Authority Info Access

Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)

Alternative Name:

URL=**http://ocsp.br-edv.brnet.int/ocsp**

4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen

Der OCSP-Dienst kann nach eigenem Ermessen der Zertifikatsprüfer genutzt werden.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Es werden keine weiteren Formen zur Anzeige von Sperrinformationen angeboten.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Bei Kompromittierung des privaten Schlüssels der **RfA Issuing-CA**, eines Endnutzers oder -systems wird das zugehörige Zertifikat unverzüglich nach Bekanntwerden der Kompromittierung oder eines hinreichenden Verdachts darauf gesperrt.

Nach einer Sperrung wegen der mutmaßlichen Kompromittierung eines privaten Schlüssels informiert die **RfA Issuing-CA** unverzüglich das Security-Management der **RfA** über den Sachverhalt. Dieses kann daraufhin nach eigenem Ermessen einen Security-Incident-Prozess einleiten.

4.9.13 Bedingungen für eine Suspendierung

Eine temporäre Sperrung bzw. eine Suspendierung von Zertifikaten wird nicht angeboten.

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 **RfA Issuing-CA** bietet **RfA**-intern einen OCSP Online-Statusabfrage-Dienst an (vgl. Kapitel 4.9.9).

4.10.1 Funktionsweise des Statusabfragedienstes

Der angebotene Statusabfragedienst unterstützt OCSP nach RFC 5019.

4.10.2 Verfügbarkeit des Statusabfragedienstes

Es wird keine Mindestverfügbarkeit des OCSP-Dienstes zugesichert.

4.10.3 Optionale Leistungen

Entfällt.

4.11 Kündigung durch den Zertifikatsnehmer

Bei einer Beendigung des Arbeitsvertrags durch einen menschlichen Zertifikatsnehmer werden dessen persönliche Zertifikate von der **RFA Issuing-CA** gesperrt. Dasselbe gilt, falls der **RFA Issuing-CA** durch die zuständige Personalabteilung, den Zertifikatsnehmer selbst oder dessen Vorgesetzten gemeldet wird, dass der Zertifikatsnehmer ohne Kündigung des Arbeitsvertrags eine andere Stelle übernimmt, bei der er die betreffenden persönlichen Zertifikate nicht mehr benötigt.

Analog dazu wird bei einer Betriebseinstellung bzw. De-Inventarisierung eines technischen Systems als Zertifikatsnehmer dessen Zertifikat gesperrt, wenn der Zertifikatsverantwortliche für das technische System einen entsprechenden Sperrantrag stellt oder dies auf andere Weise der CA zur Kenntnis gelangt.

4.12 Schlüsselhinterlegung und Wiederherstellung

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.

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel

Die **RFA Issuing-CA** bietet eine zentrale Schlüsselhinterlegung für S/MIME-Verschlüsselungszertifikate an. Eine Schlüsselhinterlegung für Authentisierungs- und Signaturschlüssel von Benutzern erfolgt nicht.

Dazu wird die Key Archival Funktion der Microsoft Active Directory Certificate Services genutzt:

Der Private-Key wird zusammen mit dem Zertifikatsrequest an die **RfA Issuing-CA** übermittelt, dort geprüft und verschlüsselt mit den Keys mehrerer Key Recovery Agents zentral gespeichert.

Im Bedarfsfall kann einer der Certificate Manager des verschlüsselten Private-Key exportieren und an einen der Key Recovery Agents weiterleiten. Dieser entschlüsselt den Private Key und leitet ihn als importierbare PKCS#12 Datei an den berechtigten Antragsteller weiter. Die Passphrase für die PKCS#12-Datei wird separat übermittelt.

Die privaten Schlüssel der Key Recovery Agents sind auf PIN-geschützten Smartcards gespeichert.

Die Key Recovery Agents sind nicht Mitglieder der PKI-Administration, sondern aus den folgenden Teams der **RfA**:

- Personalrat
- Datenschutz

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Eine Wiederherstellung von Sitzungsschlüsseln wird nicht angeboten.

5. Nicht-technische Sicherheitsmaßnahmen

Die Gewährleistung geeigneter infrastruktureller, organisatorischer und personeller Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb einer PKI.

Die **RfA-Issuing-CA(s)** werden grundsätzlich nach den gleichen Vorgaben und in der gleichen Infrastruktur, Räumlichkeiten etc. betrieben wie IT-Systeme **der RfA** mit vergleichbar hohem Schutzbedarf, bspw. Active Directory Domain Controller. Daher kann davon ausgegangen werden, dass die einschlägigen Sicherheitsmaßnahmen in der Bewertung **der RfA** grundsätzlich hinreichend sicher für den Betrieb einer PKI sind. Die diesbezüglichen Vorgaben sind innerhalb **der RfA** separat geregelt und nicht Teil dieses Policy-Dokuments.

Nachfolgend werden daher insbesondere Sicherheitsmaßnahmen beschrieben, die speziell den Betrieb der **RFA Issuing-CA(s)** betreffen.

5.1 Bauliche Sicherheitsmaßnahmen

5.1.1 Lage und Gebäude

Die virtuelle Maschine der **RfA-Issuing-CA** wird auf einem Hypervisor-Cluster betrieben, das physisch in den Rechenzentrumsräumen der **RfA** in München untergebracht ist. Die eingesetzten physischen Sicherheitsvorkehrungen gewährleisten einen hinreichenden Schutz vor äußeren Einflüssen (vgl. die Vorbemerkung zu Kapitel 5).

5.1.2 Zugang

Die Rechenzentrumsräume, in denen die **RFA Issuing-CA** betrieben wird, ist durch geeignete physische Sicherheitsvorkehrungen geschützt, der den Zutritt nur für berechtigte Mitarbeiter **der RfA** oder ihrer ständig beauftragten Dienstleister bzw. für Notfallpersonal ermöglicht. Mitarbeiter von sonstigen Fremdfirmen dürfen nur in Begleitung eines berechtigten Mitarbeiters diese Räumlichkeiten betreten.

Die Zutrittsregelungen im Detail sind durch **die RfA** an anderer Stelle geregelt (vgl. die Vorbemerkung zu Kapitel 5).

5.1.3 Strom, Heizung und Klimaanlage

Stromversorgung und ausreichende Klimatisierung sind in den Räumlichkeiten, in denen die **RFA Issuing-CA** betrieben wird, durch geeignete Maßnahmen sichergestellt (vgl. die Vorbemerkung zu Kapitel 5).

5.1.4 Wassergefährdung

Gefährdungen durch Wasser sind hinreichend ausgeschlossen (vgl. die Vorbemerkung zu Kapitel 5).

5.1.5 Brandschutz

Im Serverraum ist ein geeigneter Brandschutz implementiert (vgl. die Vorbemerkung zu Kapitel 5).

Backup- und Disaster-Recovery-Daten der PKI (vgl. Kapitel 5.1.8) werden als Kopie in zwei Tresoren aufbewahrt.

5.1.6 Lager und Archiv

Datenträger mit sicherheitsrelevanten, vertraulichen oder personenbezogenen Daten werden verschlüsselt und/oder vor unberechtigten Zugriffen geschützt aufbewahrt (vgl. die Vorbemerkung zu Kapitel 5).

5.1.7 Datenvernichtung

Bei der Entsorgung von Papierdokumenten und elektronischen Datenträgern ist durch separate Regelungen sichergestellt, dass alle sicherheitsrelevanten, vertraulichen oder personenbezogenen Daten ordnungsgemäß vernichtet werden (vgl. die Vorbemerkung zu Kapitel 5).

Für Datenträger und besonders Schlüsselmaterial wird dabei die höchste innerhalb der RfA angebotene Sicherheitsstufe der Entsorgung gewählt, die die physische Zerstörung von Datenträgern und Geräten einschließt.

5.1.8 Disaster Backup

Zu Disaster-Recovery-Zwecken werden das jeweils neuste komplette System-Backup der **RFA Issuing-CA**, eine Sicherheitskopie der **RFA Issuing-CA** Schlüssel und die zugehörigen Credentials bzw. Aktivierungsdaten sicher aufbewahrt.

- Backup-System: Backup-System der **RfA** für virtuelle Maschinen
- Schlüssel und Passwortbriefe: Safe der IT-Sicherheit und Safe der IT-Basis-Infrastruktur

Das Systembackup der **RFA Issuing-CA** unterliegt denselben Zugriffschutzmechanismen und demselben Verfügbarkeitsniveau wie ein System-Backup der Domänen-Controller des Active Directory **der RfA**, so dass von einem angemessenen Schutzniveau auszugehen ist (vgl. die Vorbemerkung zu Kapitel 5).

5.2 Verfahrensvorschriften

5.2.1 Rollenkonzept

Für Installation, Konfiguration und Betrieb der **RfA Issuing-CA(s)** sowie ggf. deren Wiederherstellung aus dem Backup sind folgende Rollen definiert und umgesetzt:

Rolle	Typ der Rolle	Mindestanzahl Personen	Aufgaben
Partition Owner des HSM (PO)	HSM	1	Erstellen und Nutzung des CA-Schlüssels in der Partition der **RfA Issuing-CA** des HSM Technische Rolle, zur automatischen Nutzung hinterlegt im Server der CA, verwaltet durch den lokalen Administrator des **RFA Issuing-CA** Systems
Lokaler Administrator des **RFA Issuing-CA** Systems	Betriebssystem	2	Administration des Betriebssystems Installation der AD Certificate Services Backup und Restore der CA
RFA Issuing-CA Administrator	PKI	2	Betreibt, konfiguriert und wartet die CA, Erstellt, korrigiert und verwaltet die Zertifikatstemplates der CA und weist die PKI-bezogenen Rechte zu.
RFA Issuing-CA Certificate Manager	PKI	2	Ist verantwortlich für die Zertifikatsausstellung und ggf. -sperrung.
Key Recovery Agent	PKI	2	Kann die zentral hinterlegten Private-Keys von Verschlüsselungszertifikaten entschlüsseln (bekommt jedoch erst im Bedarfsfall Zugriff auf einzelne verschlüsselte Keys).
Tresorverwalter für Safe der IT-Sicherheit	Schließregelung	1	Zugriff auf Safe der IT-Sicherheit. Dort werden verwahrt: 1. Versiegelte Umschläge mit dem zweigeteilten SO (HSM-Administrator) Passwort des HSM

			2. Versiegelte Umschläge mit dem zweigeteilten Backup-Wrapping-Key des HSM. 3. Versiegelter Umschlag mit dem PO (API-User) Passwort für die HSM-Partition der CA 4. Versiegelter Umschlag mit dem Wrapping-Key-verschlüsselten Schlüsselmaterial des HSM auf USB-Stick 5. Versiegelter Umschlag mit dem Auditor-Passwort des HSM 6. Versiegelte Umschläge mit PIN und Admin-Key einer produktiv genutzten Key-Recovery-Agent-Smartcard 7. Versiegelte Umschläge mit einer Reserve-Key-Recovery-Agent-Smartcard sowie deren PIN und Admin-Key
Tresorverwalter für Safe der IT-Basis-Infrastruktur	Schließregelung	1	Zugriff auf den Safe der IT-Basis-Infrastruktur. Dort werden verwahrt: 1. Versiegelte Umschläge mit dem zweigeteilten SO (HSM-Administrator) Passwort des HSM 2. Versiegelte Umschläge mit dem zweigeteilten Backup-Wrapping-Key des HSM. 3. Versiegelter Umschlag mit dem PO (API-User) Passwort für die HSM-Partition der CA 4. Versiegelter Umschlag mit dem Wrapping-Key-verschlüsselten

			Schlüsselmaterial des HSM auf USB-Stick 5. Versiegelter Umschlag mit dem Auditor-Passwort des HSM 6. Versiegelte Umschläge mit PIN und Admin-Key einer produktiv genutzten Key-Recovery-Agent-Smartcard 7. Versiegelte Umschläge mit einer Reserve-Key-Recovery-Agent-Smartcard sowie deren PIN und Admin-Key

Die Rolle des Security Officers des HSM (SO, HSM-Administrator) ist eine Rolle der Offline **RfA-CA** und in deren CPS beschrieben.

5.2.2 Mehraugenprinzip

Bei der Wiederherstellung von hinterlegten Verschlüsselungsschlüsseln (vgl. Kapitel 4.12) wird ein Vier-Augen-Prinzip wie folgt umgesetzt:

- Nur Certificate Manager oder CA-Administratoren haben Zugriff auf die verschlüsselten hinterlegten Private-Keys. Sie können sie jedoch nicht entschlüsseln, sondern nur im Bedarfsfall einem Key Recovery Agent übermitteln.
- Key Recovery Agents können hinterlegte Private-Keys entschlüsseln, haben aber ohne Mitwirkung eines Certificate Managers oder CA-Administrators keinen Zugriff auf die verschlüsselten Keys.
- Zwischen diesen beiden Rollen herrscht eine Rollentrennung,

Darüber hinaus wird kein Mehraugenprinzip verwendet.

5.2.3 Identifizierung und Authentifizierung jeder Rolle

Zur Authentifizierung bei allen Rollen genügt eine Ein-Faktor-Authentifizierung, wie bspw. Benutzername und Passwort entsprechend der aktuell gültigen Passwortrichtlinie **der RfA**.

Key Recovery Agents nutzen eine Smartcard und deren PIN zur Authentifikation.

5.2.4 Rollentrennung

Die Rollen der Tresorverwalter und Key Recovery Agents sind unvereinbar mit den anderen in Kapitel 5.2.1 aufgeführten Rollen. Alle übrigen Rollen können, müssen aber nicht in Personalunion durch dieselben Personen wahrgenommen werden.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

Die CA-Administratoren der **RFA Issuing-CA** kennen den Stand der Technik und die Best Practices im Bereich Zertifikatsinfrastruktur. Dies weisen sie durch den Besuch einer entsprechenden Schulung oder auf andere geeignete Weise nach.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Eine Sicherheitsüberprüfung der CA-Administratoren ist nicht erforderlich.

5.3.3 Anforderungen an Schulungen

Für CA-Administratoren der **RFA Issuing-CA** bestehen keine Anforderungen an bestimmte Schulungen als CA-Administrator. Sie sind jedoch gehalten, ihre Kenntnisse auf dem aktuellen Stand der Technik im Bereich Zertifikatsinfrastruktur zu halten.

5.3.4 Häufigkeit von Schulungen und Belehrungen

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

5.3.5 Häufigkeit und Folge von Job-Rotation

Es finden keine Job-Rotationen statt.

5.3.6 Maßnahmen bei unerlaubten Handlungen

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

5.3.7 Anforderungen an freie Mitarbeiter

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

5.3.8 Dokumente, die dem Personal zur Verfügung gestellt werden müssen

Den CA-Administratoren der **RFA Issuing-CA** wird das Certificate Policy Dokument mit den Mindestanforderungen der **RFA-CA** an die untergeordneten Issuing-CAs zur Verfügung gestellt.

5.4 Überwachungsmaßnahmen

5.4.1 Arten von aufgezeichneten Ereignissen

Alle sicherheitsrelevanten Ereignisse der **RfA Issuing-CA** werden in Log-Dateien protokolliert. 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

Die Ereignisse sind über das Windows-Event-Log im „Security“-Log einsehbar. Die Log Größe ist auf 192 MB beschränkt, ältere Einträge werden bei Erreichen der Größenbegrenzung aus dem Log gelöscht.

Zusätzlich wird bei den einzelnen Typen von sicherheitsrelevanten Ereignissen jeweils eine E-Mail an ein Postfach der PKI-Administration gesendet, in dem sie für mindestens sieben Tage aufbewahrt wird.

Zusätzlich werden die Windows Log-Events an das SIEM (Security Information and Event Management) System der RfA weitergeleitet und nach den dafür geltenden separaten Regelungen ausgewertet und aufbewahrt (vgl. die Vorbemerkung zu Kapitel 5). Es kann davon ausgegangen werden, dass die Sicherungszeit mindestens sieben Tage beträgt.

5.4.2 Häufigkeit der Bearbeitung der Aufzeichnungen

Nur bei begründeten Verdachtsmomenten auf Missbrauch der **RFA Issuing-CA** wird eine anlassbezogene Prüfung der Log-Protokolle (Aufzeichnungen) durchgeführt.

5.4.3 Aufbewahrungszeit von Aufzeichnungen

Die Log-Aufzeichnungen der **RFA Issuing-CA** werden für mindestens 7 Tage aufbewahrt (vgl. Kapitel 5.4.1).

5.4.4 Sicherung der Aufzeichnungen

Die Protokolldaten (Aufzeichnungen) sind ausreichend gegen unberechtigten Zugriff, Löschung und Manipulation geschützt. Zugriff auf die Server **der RFA** hat nur der nach separaten Regelungen definierte Personenkreis der Serveradministratoren (vgl. die Vorbemerkung zu Kapitel 5).

5.4.5 Datensicherung der Aufzeichnungen

Das lokale Log-Protokoll der **RFA Issuing-CA** wird als Teil des Systembackups regelmäßig gesichert. Die Sicherung richtet sich nach den allgemeinen Vorgaben der RfA für die betreffende Systemplattform (vgl. die Vorbemerkung zu Kapitel 5).

Die an das **SIEM** System weitergeleiteten Events werden nach den dafür geltenden separaten Regelungen gesichert (vgl. die Vorbemerkung zu Kapitel 5). Es kann davon ausgegangen werden, dass die Sicherungszeit mindestens sieben Tage beträgt.

5.4.6 Speicherung der Aufzeichnungen (intern / extern)

Die Speicherung des Log-Protokolls (Aufzeichnungen) erfolgt lokal und optional im SIEM-System.

5.4.7 Benachrichtigung der Ereignisauslöser

Keine weiteren Festlegungen.

5.4.8 Schwachstellenanalyse

Die **RFA Issuing-CA** ist in das allgemeine Patch-Management **der RfA** aufgenommen (vgl. die Vorbemerkung zu Kapitel 5). Schwachstellen bei den eingesetzten Systemen werden nach Bekanntwerden der Schwachstelle und Vorliegen eines Patches umgehend geschlossen.

Bei Hinweisen des Herstellers der eingesetzten HSMs auf sicherheitsrelevante Updates der HSM-Software sind die CA-Administratoren dafür verantwortlich, die betreffenden Schwachstellen zu bewerten und ggf. die Updates/Patches einzuspielen.

Die Verantwortlichen für den PKI-Betrieb haben die Organisationseinheit, die für den Betrieb des SIEM verantwortlich ist, über die Bedeutung der an das SIEM weitergeleiteten Meldungen der CA informiert und stehen für Rückfragen zur Verfügung.

Die Auswertung der weitergeleiteten Meldungen durch das SIEM liegt in der Verantwortlichkeit des SIEM-Teams (vgl. die Vorbemerkung zu Kapitel 5).

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen

Die folgenden Daten werden archiviert:

- Zweigeteiltes SO (HSM-Administrator) Passwort des HSM
- Zweigeteilter Backup-Wrapping-Key des HSM.
- PO (API-User) Passwort für die HSM-Partition der CA
- Mit dem Wrapping-Key verschlüsseltes Schlüsselmaterial des HSM

5.5.2 Aufbewahrungsfristen für archivierte Daten

Die in Kapitel 5.5.1 genannten Daten werden über die gesamte Betriebsdauer der **RfA-Issuing-CA**-aufbewahrt.

5.5.3 Sicherung des Archivs

Die genannten Daten werden in einem Tresor verschlossen aufbewahrt. Sie sind in verschlüsselter Form oder innerhalb des Tresors in versiegelten Umschlägen hinterlegt.

Durch diese Art der Aufbewahrung sind sie angemessen gegen unberechtigten Zugriff geschützt.

5.5.4 Datensicherung des Archivs

Es erfolgt keine gesonderte Sicherung des Archivs.

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

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

5.5.6 Archivierung (intern / extern)

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

5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen

Entfällt.

5.6 Schlüsselwechsel der CA

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

Beim Schlüsselwechsel einer **RfA-Issuing-CA** wird neues Schlüsselmaterial generiert.

5.7 Kompromittierung und Geschäftsweiterführung

5.7.1 Behandlung von Vorfällen und Kompromittierungen

Bei Verlust des **RfA-Issuing-CA** Schlüssels durch Systemausfall oder Löschung der Daten kann der **RfA-Issuing-CA** Schlüssel aus der Sicherungskopie (vgl. Kapitel 5.5) wiederhergestellt werden.

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

Bei sonstigen Verdachtsfällen einer Kompromittierung der **RfA-Issuing-CA** wird der IT-Sicherheitsbeauftragte der **RfA** informiert, der über das weitere Vorgehen 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.

Im konkreten Fall wird nach den Vorgaben des IT-Sicherheitsbeauftragten der **RfA** darüber entschieden, welche Art der Datensicherung als unkompromittiert gelten kann und wie die Wiederherstellung erfolgt. Ggf. kann das System unter Rückgriff auf den hinterlegten CA-Schlüssel komplett neu aufgebaut werden.

5.7.3 Verhalten bei Kompromittierung des privaten Schlüssels der CA

Bei hinreichendem Verdacht auf eine Kompromittierung des privaten Schlüssels der **RfA-Issuing-CA** wird unverzüglich die Sperrung des **RfA-Issuing-CA** Zertifikats bei der **RfA-CA** beantragt. Danach können auf einem unkompromittierten bzw. bereinigten System neue Schlüssel erzeugt und ein neues CA-Zertifikat beantragt werden.

5.7.4 Möglichkeiten zur Geschäftsweiterführung nach einer Kompromittierung

Die Wiederaufnahme des Betriebs nach einem Disaster sollte nach Möglichkeit ohne Datenverlust erfolgen. Hierzu werden im Bedarfsfall alle als Backup, archiviert oder an anderer Stelle verfügbaren, nicht-kompromittierten Daten genutzt, z. B. Backups von Log-Dateien, publizierte Sperrlisten und Zertifikate, Backups der CA-Datenbank.

Über die genaue Art der Wiederherstellung wird im konkreten Einzelfall im Einvernehmen mit dem IT-Sicherheitsbeauftragten der **RfA** entschieden.

5.8 Schließung einer CA oder einer Registrierungsstelle

Wenn eine **RfA-Issuing-CA** ihren Betrieb einstellt, wird deren CA-Zertifikat - sofern nicht bereits abgelaufen - durch die **RfA-CA** gesperrt. Dadurch werden auch die von ihr ausgestellten Zertifikate invalidiert und dafür gesorgt, dass der private Schlüssel der CA im Anschluss nicht missbräuchlich verwendet werden kann.

Wenn eine Betriebsgruppe oder Management-System, das RA-Funktionen übernimmt (bspw. ein MDM) seinen Betrieb einstellt, werden die dafür genutzten Zugangsdaten (Passwörter und/oder Zertifikate) gesperrt und die entsprechenden Berechtigungen in der CA-Software entzogen.

6. Technische Sicherheitsmaßnahmen

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

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

Das Schüsselpaar der **RfA-Issuing-CA** wurde in einem HSM erzeugt und gespeichert (vgl. Kapitel 6.2).

Die Schlüsselerzeugung durch Endanwender und Endsysteme muss sich nach deren technischen Gegebenheiten richten und liegt in der Verantwortung der jeweiligen Zertifikatsinhaber bzw. Zertifikatsverantwortlichen. Die **RfA-Issuing-CA** kontrolliert vor einer Zertifikatserstellung stets die Einhaltung der in diesem Dokument geforderten Kryptoalgorithmen und Mindestschlüssellängen.

Eine zentrale Erzeugung von Schlüsselpaaren für Endanwender bei der **RfA-Issuing-CA** findet nicht statt.

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Eine Übermittlung des privaten Schlüssels an einen Zertifikatsnehmer oder eine RA ist nicht notwendig und wird nicht angeboten.

6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

Der Zertifikatsantrag der **RfA-Issuing-CA** mit dem zu zertifizierenden öffentlichen Schlüssel an die CA-Administratoren der **RfA-CA** über einen Transfer-Datenträger oder per E-Mail übermittelt.

Die öffentlichen Schlüssel von Endanwendern werden an die **RfA Issuing-CA** als Zertifikatsantrag über eine der in Kapitel 4.2.2 genannten technischen Schnittstellen übermittelt. Jede dieser Schnittstellen beinhaltet eine Authentisierung des berechtigten Antragstellers bzw. technischen Systems oder eine direkte Validierung der im Zertifikat beantragten Namensinformation.

In allen Fällen ist der Zertifikatsantrag, der den öffentlichen Schlüssel enthält, mit dem zugehörigen Privat-Key signiert. Diese digitale Signatur wird durch die empfangende CA geprüft und so sichergestellt, dass der Ersteller des Antrags im Besitz dieses Private-Keys ist.

6.1.4 Lieferung öffentlicher Schlüssel der CA an Zertifikatsnutzer

Die **RfA-Issuing-CA** stellt ihr eigenes Issuing-CA-Zertifikat den Zertifikatsprüfern über die in Kapitel 2.1 genannten Verzeichnisse zur Verfügung, so dass es automatisch von einer Anwendung zu Verifikationszwecken heruntergeladen und verwendet werden kann.

6.1.5 Schlüssellängen

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

Endanwender-Schlüssel nutzen ebenfalls das RSA-Verfahren. Die Schlüsselpaare der Endnutzer oder -systeme sollen bei Neuausstellung grundsätzlich 4096 Bit lang sein. Im Ausnahmefall bei Endsystemen, die diese Schlüssellänge technisch nicht unterstützen, wird eine Schlüssellänge ab mindestens 2048 Bit akzeptiert.

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

- P-256, Schlüssellänge 256 Bit [6]

6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle

Das Schlüsselpaar der **RfA Issuing-CA** wurde in einem HSM generiert, das nach FIPS 140-2 zertifiziert ist und die entsprechenden Vorgaben zur Schlüsselgenerierung einhält.

Auch die Public Key Parameter der Schlüsselpaare von Endanwendern sollen den Anforderungen aus FIPS 140-2 oder einem vergleichbaren Standard entsprechen. Die Einhaltung dieser Anforderung ist jedoch bei Schlüsseln, die dezentral generiert werden, vom jeweiligen Endsystem abhängig und kann von der **RfA Issuing-CA** jedoch über die Prüfung der erforderlichen Mindestschlüssellänge hinaus nicht effektiv geprüft werden.

Das gleiche gilt für Schlüssel auf Basis elliptischer Kurven, die in Endanwenderzertifikaten alternativ genutzt werden dürfen. Als Parameter für solche Schlüssel sind die folgenden Named-Curves zulässig:

- P-256 alias secp256r1 (OID: 1.2.840.10045.3.1.7)

6.1.7 Schlüsselverwendungen

Alle von der **RfA-Issuing-CA** ausgestellten Zertifikate sowie die zugehörigen privaten Schlüssel dürfen nur zu den in den Zertifikaten spezifizierten Verwendungszwecken eingesetzt werden (siehe Kapitel 7.1.2).

Zertifikatsprüfer (Relying Parties) sind verpflichtet, diese Schlüsselverwendungszwecke zu prüfen, bevor sie das Zertifikat verwenden. Die Einhaltung dieser Anforderung kann durch die **RfA-Issuing-CA** jedoch nicht effektiv kontrolliert werden.

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

Die für die Schlüssel der **RfA Issuing-CA** verwendeten Hardware-Sicherheitsmodule (YubiHSM 2) sind nach FIPS 140-2 Level 3 zertifiziert.

Die privaten Schlüssel vom Key Recovery Agents, mit denen zentral hinterlegten Endanwenderschlüssel entschlüsselt werden können, sind auf Smartcards gespeichert, die nach FIPS 104-2 oder einem gleichwertigen Common Criteria Protection Profile zertifiziert sind.

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

Der administrative Zugriff auf das HSM der **RfA Issuing-CA** erfordert eine Anmeldung nach dem Mehraugenprinzip (2-von-2). Der Backup/Wrapping-Key des HSM ist ebenfalls nach dem Mehraugenprinzip (2-von-2) aufgeteilt hinterlegt.

Darüber hinaus wird kein Mehraugenprinzip eingesetzt.

6.2.3 Hinterlegung privater Schlüssel

Die **RfA-Issuing-CA** bietet eine Schlüsselhinterlegung ausschließlich für Verschlüsselungszertifikate an. Die dabei eingesetzten Verfahren und Prozesse sind in Kapitel 4.12 beschrieben.

6.2.4 Sicherung privater Schlüssel

Der im HSM gespeicherte private Schlüssel der **RfA-Issuing-CA** wird für einen möglichen Recovery-Fall in Dateiform verschlüsselt mit dem Backup-Wrapping-Key auf USB Datenträgern gesichert.

Der Wrapping-Key selbst wird - nach dem Mehraugenprinzip verteilt (siehe Kapitel 6.2.2) - ebenfalls für den Recovery-Fall gesichert.

Die einzelnen Teile des Wrapping-Keys sind in separat versiegelten Umschlägen gespeichert.

Zusätzlich ist der private Schlüssel der RfA Issuing-CA in einem weiteren HSM gespeichert, das im Regelfall von der RfA-CA genutzt wird.

6.2.5 Archivierung privater Schlüssel

Die in diesem Kapitel genannten notierten Schlüssel und Credentials in versiegelten Umschlägen sowie die genannten Datenträger/Hardware mit Schlüsselmaterial sind vor unberechtigtem Zugriff geschützt in den folgenden Tresoren hinterlegt:

- Safe der IT-Sicherheit
- Safe der IT-Basis-Infrastruktur

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Die im HSM gespeicherten CA-Schlüssel können nicht in unverschlüsselter Form aus dem HSM exportiert werden.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Für Schlüssel der CA gelten die Regelungen aus Kapitel 6.2.1.

Endanwendern und Systemen steht es frei, ihre privaten Schlüssel in Smartcard oder HSM oder in Software zu speichern.

6.2.8 Aktivierung privater Schlüssel

Die Aktivierungsdaten für die HSM-Partition, welche die Schlüssel der **RFA Issuing-CA** enthält, werden durch den HSM-Administrator (Security Officer, diese Rolle wird von den CA-Administratoren mit übernommen) vergeben. Sie sind auf dem Serversystem der CA hinterlegt, damit die HSM-Partition nach dem Systemstart automatisch aktiviert wird.

Die genaue Art der Aktivierung privater Schlüssel von Endanwendern und Systemen richtet sich nach der technischen Funktionalität der jeweiligen Anwendung bzw. Systemplattform. Die privaten Schlüssel der Endanwender werden bei Speicherung in Software durch eine Benutzeranmeldung gemäß den Sicherheitsvorgaben **der RfA** oder bei Speicherung in Hardware mittels einer mindestens vierstelligen PIN vor unautorisiertem Zugriff geschützt. Der Zugriff auf den privaten Schlüssel von Systemen wird nicht zwingend durch ein Passwort gesichert. Der Zugriff auf Systeme ist gemäß den Sicherheitsvorgaben **der RfA** geschützt.

6.2.9 Deaktivierung privater Schlüssel

Bei Bedarf können die CA-Administratoren der **RfA-CA** in ihrer Teilrolle als HSM-Administrator (SO) die für die entsprechende HSM-Partition vergebenen Aktivierungsdaten löschen bzw. invalidieren und somit den darin gespeicherten privaten CA-Schlüssel deaktivieren.

Die genaue Art der Deaktivierung privater Schlüssel von Endanwendern und Systemen richtet sich nach der technischen Funktionalität der jeweiligen Anwendung bzw. Systemplattform. Sofern technisch keine andere Art der Deaktivierung möglich ist, kann der Endanwender durch Abmelden bzw. der Systemverantwortliche durch Herunterfahren des Systems den privaten Schlüssel deaktivieren.

6.2.10 Zerstörung privater Schlüssel

Private Schlüssel der **RfA Issuing-CA** werden, bei Bedarf und nur nachdem zuvor das betreffende CA-Zertifikat gesperrt wurde oder abgelaufen ist, mit der geprüften Lösch-Funktion des HSMs von allen HSMs, auf denen der Schlüssel gespeichert ist (auch Backup-HSMs) gelöscht.

Hinterlegte Sicherheitskopien der CA-Schlüsseln auf Datenträgern sowie zugehörige Keys bzw. Passwörter oder PINs in versiegelten Umschlägen werden dem jeweiligen Tresor entnommen und entsprechend der Datenschutz-Vorgaben **der RfA** für personenbezogene Daten vernichtet und entsorgt.

Die genaue Art der Deaktivierung privater Schlüssel von Endanwendern und Systemen richtet sich nach der technischen Funktionalität der jeweiligen Anwendung bzw. Systemplattform. Sofern private Schlüssel von Endanwendern oder Systemen bei Bedarf nach Löschung des Schlüssels technisch bedingt oder wegen Verlust eines Geräts nicht sicher gelöscht werden können und das zugehörige Zertifikat nicht abgelaufen ist, sind die Endanwender bzw. Systemverantwortlichen verpflichtet, die Sperrung des Zertifikats zu beantragen.

Um den privaten Schlüssel eines Anwenders auf einer Smartcard zu löschen, wird diese bei Bedarf entsprechend der Datenschutz-Vorgaben **der RfA** für personenbezogene Daten vernichtet und entsorgt.

6.2.11 Beurteilung kryptographischer Module

Siehe Abschnitt 6.2.1.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Entfällt.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Das CA-Zertifikat der **RfA-Issuing-CA** ist 10 Jahre gültig. Der private Schlüssel der **RfA-Issuing-CA** wird jedoch nur solange zur Ausstellung neuer untergeordneter Zertifikate verwendet werden, wie das Gültigkeitsende der ausgestellten Zertifikate noch im Gültigkeitsbereich der **RfA-Issuing-CA** liegt.

Endanwenderzertifikate haben eine maximale Laufzeit von 5 Jahren.

OCSP-Signing-Zertifikate haben eine maximale Laufzeit von 30 Tagen.

6.4 Aktivierungsdaten

6.4.1 Aktivierungsdaten

Die CA-Administratoren und Certificate Manager der **RfA-Issuing-CA** verwenden zur Anmeldung sichere Passwörter entsprechend der Passwort-Richtlinie **der RfA**.

6.4.2 Schutz von Aktivierungsdaten

Die betreffenden Passwörter sind nur den CA-Administratoren bzw. Certificate Managern der **RfA-Issuing-CA** selbst und ggf. - soweit nach Passwort-Richtlinie **der RfA** zulässig - ihren Vertretern bekannt.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Die **RfA-Issuing-CA** wird auf einem Windows Server 2022 betrieben, auf den nur nach einer Benutzeranmeldung mit einem autorisierten Benutzerkonto zugegriffen werden kann.

Das System ist nach den Vorgaben der Microsoft Security Baseline für Windows 2022 Member Server gehärtet. In den folgenden Punkten wird begründet von der Microsoft-Härtungsvorgabe abgewichen:

- Auf Einstellungen, die nicht primär der Sicherheit dienen, sondern der Telemetrie und Datenweitergabe an Microsoft (z. B. Feedback-Programme) wurde verzichtet.
- Einstellungen zur virtualisierungsbasierten Sicherheit wurden deaktiviert, da diese innerhalb einer virtuellen Maschine nicht nutzbar sind und u. U. zu technischen Problemen führen.
- Die Kennwortrichtlinie entspricht der Passwort-Richtlinie **der RfA** im Active Directory.
- Die Einstellungen zum Malware-Schutz richten sich nach den Sicherheitsvorgaben **der RfA** und nicht nach den Microsoft-Baseline-Einstellungen für den Microsoft Defender.

- Die Einstellungen zu Anmeldebeschränkungen (lokal und per Netzwerk) sind an die etablierte Arbeitsweise der CA-Administratoren bei **der RfA** angepasst.

6.5.2 Beurteilung von Computersicherheit

Keine weiteren Festlegungen.

6.6 Technische Maßnahmen während des Life Cycles

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

Keine weiteren Festlegungen.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Die Serversysteme der **RfA-Issuing-CA** sowie die Virtualisierung-Infrastruktur sind in den regelmäßigen Patch- und Update- Managementprozess **der RfA** integriert.

Die CA-Administratoren der **RfA Issuing-CA** sind dafür verantwortlich, sich regelmäßig, mindestens einmal pro Monat, über Schwachstellen des eingesetzten HSM oder der damit verbundenen Software zu informieren, eventuelle neue Schwachstellen zu bewerten und ggf. Hersteller-Patches dagegen einzuspielen.

Bei Schwachstellen mit einer CVSS-Bewertung von 7.0 oder höher, die im Einsatzszenario bei der CA relevant sind, werden Hersteller-Patches unverzüglich eingespielt.

6.6.3 Sicherheitsmaßnahmen während der Life Cycles

Für die Systeme der **RfA-Issuing-CA**, die virtuelle Infrastruktur der **RfA** und die HSMs gelten während des Lebenszyklus die gleichen Sicherheitsmaßnahmen wie für alle anderen Serversysteme der **RfA** auch.

6.7 Sicherheitsmaßnahmen für Netze

Die Systeme der **RfA-Issuing-CA(s)** sind vor unberechtigten Zugriffen per Netzwerk und vor Zugriffen von außen geschützt.

Dazu werden die folgenden Sicherheitsmechanismen eingesetzt:

- Die Systeme werden im internen Netz **der RfA** betrieben, das von externen Netzen wie dem Internet und dem ARD-Netz durch eine Firewall nach den Sicherheitsvorgaben **der RfA** getrennt ist. Diese Firewall erlaubt keine direkte Netzwerkverbindungen von außen auf CA-Server.
- Die Systeme werden innerhalb des internen Netzes im selben Server-Netzbereich betrieben, in dem auch vergleichbar sicherheitskritische Server angesiedelt sind. Dieser Netzbereich ist entsprechend der Sicherheitsvorgaben **der RfA** auch aus den anderen Bereichen des internen Netzes nur über eine Firewall-Filterung zu erreichen.
- Zur Verbindung eines CA-Servers mit dem USB-basierten YubiHSM wird ein USB-Device-Server verwendet, über den per Netzwerk auf das dort eingesteckte USB-HSM zugegriffen werden kann. Die Vertraulichkeit und Integrität dieser Netzverbindung wird unabhängig vom USB-Device-Server dadurch gewährleistet, dass alle übertragenen Nachrichten per Secure Messaging zwischen der HSM-Middleware auf dem CA-Server und dem HSM

geschützt werden. Eine Störung der Netzverbindung wird durch die Betriebsüberwachung der CA zeitnah entdeckt und durch die zuständigen Administratoren unverzüglich behoben.

- Wie vom Härtungsprofil (vgl. Kapitel 6.5.1) vorgegeben, ist auf den Windows-Servern die Windows Defender Firewall aktiv.

6.8 Zeitstempel

In der **RfA** wird kein Zeitstempeldienst betrieben.

7. Profile von Zertifikaten, Sperrlisten und OCSP

7.1 Zertifikatsprofile

7.1.1 Versionsnummern

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

7.1.2 Zertifikatserweiterungen

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

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

Die KeyUsage wird als kritisch, alle anderen als nicht-kritisch markiert. Optional werden je nach Zertifikatstyp außerdem eine kritische BasicConstraints-Erweiterung und weitere nicht kritische Zertifikatserweiterungen in den Zertifikaten für Endanwender und Systeme ergänzt, wie bspw.

- SubjectAlternativeName (Alternativer Antragstellername)
- AuthorityInfoAccess (Zugriff auf Stelleninformationen)
- ExtendedKeyUsage (Erweiterte Schlüsselverwendung)
- CertificatePolices (Zertifikatrichtlinien)
- Microsoft Application Policies Erweiterung
- Microsoft Security Identifier Erweiterung

Um WLAN-Clientzertifikate für die Anmeldung am Rundfunk-WLAN RFA-übergreifend einheitlich zu kennzeichnen und sie so von anderen Client-Authentisierungszertifikaten wie bspw. VPN-Zertifikaten unterscheiden zu können, wird in allen WLAN-Clientzertifikaten für das Rundfunk-WLAN eine einheitliche „Erweiterte Schlüsselverwendung“ (X509 v3, Extended Key Usage) aufgenommen, die die Objektkennung (Object Identifier) 1.3.6.1.4.1.42638.2.1 enthält.

Um Zertifikate für die weConnect Lösung RfA-übergreifend einheitlich zu kennzeichnen und sie so von anderen Zertifikatstypen wie bspw. allgemeinen TLS-Serverzertifikaten unterscheiden zu können, wird in allen weConnect-Zertifikaten (eine einheitliche „Erweiterte Schlüsselverwendung“

(X509 v3, Extended Key Usage) aufgenommen, die die Objektkennung (Object Identifier) 1.3.6.1.4.1.42638.2.2 enthält.

Die Extended Key Usage Erweiterung wird als nicht-kritisch markiert. Es werden nur Maschinenzertifikate für Rundfunk-WLAN bzw. weConnect erstellt und stets mit der betreffenden Objektkennung in der Extended Key Usage versehen.

In den Zertifikaten für OCSP-Signing sind mindestens folgende Zertifikatserweiterungen enthalten:

- KeyUsage (Schlüsselverwendung) mit Wert "Digital Signature"
- AuthorityKeyIdentifier (Stellenschlüsselkennung)
- ExtendedKeyUsage (Erweiterte Schüsselverwendung) mit Wert OCSP Signing (1.3.6.1.5.5.7.3.9)
- OCSPNoCheck (OCSP No Revocation Check)

Die KeyUsage Erweiterung ist als kritisch, alle anderen als nicht-kritisch markiert.

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 kann alternativ auch folgendes verwendet werden:

- id-ecPublicKey (OID: 1.2.840.10045.2.1)

7.1.4 Namensformate

Siehe Kapitel 3.1.4

7.1.5 Namensbeschränkungen

Bei den **RfA-Issuing-CAs** gibt es keine Namensbeschränkungen. Die Interpretation der Namen (wie in Abschnitt 3.1.4 beschrieben) muss korrekt durchgeführt werden.

7.1.6 OIDs der Zertifikatsrichtlinien

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

Zur RFA-übergreifenden Kennzeichnung von weConnect-Zertifikaten enthalten diese eine einheitliche „Erweiterte Schlüsselverwendung“ (X509 v3, Extended Key Usage) mit der Objektkennung (Object Identifier) 1.3.6.1.4.1.42638.2.2, siehe Kapitel 7.1.2.

Zur Objektkennung dieses Dokuments siehe Kapitel 1.2.

Optional werden für einzelne Typen von Endzertifikaten weitere Objektkennungen als Policy-Identifier in einer nicht-kritischen Certificate Policies Erweiterung aufgenommen, falls dies in der

Anwendung des betreffenden Zertifikatstyps erforderlich ist oder Vorteile bietet, bspw. von Microsoft vergebene Objektkennungen, die eine Überprüfung der sicheren Schlüsselgenerierung per Key-Attestation anzeigen.

7.1.7 Nutzung der Erweiterung "Policy Constraints"

Es werden keine Beschränkungen für Sicherheitsrichtlinien (Policy Constraints) in den ausgestellten Endanwenderzertifikaten verwendet.

7.1.8 Syntax und Semantik von "Policy Qualifiers"

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

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung Zertifikatsrichtlinie

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

7.2 Sperrlistenprofile

7.2.1 Versionsnummer(n)

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

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

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

- AuthorityKeyIdentifier (Stellenschlüsselkennung)
- CRLNumber (Sperrlistennummer)

Diese Sperrlistenerweiterungen werden alle als nicht-kritisch markiert. Optional werden weitere nicht-kritische Erweiterungen in die Sperrlisten aufgenommen, bspw. NextCRLPublish (geplanter Zeitpunkt der nächsten Sperrlisten-Veröffentlichung).

7.3 Profile des Statusabfragedienstes (OCSP)

7.3.1 Versionsnummer(n)

Die **RfA Issuing-CA** bietet für die Abfrage des Sperrstatus der von ihr ausgestellten Zertifikate einen OCSP Dienst nach RFC 5019 (Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments) an.

OCSP-Responses werden mit einem delegierten OCSP-Signer-Zertifikat signiert, das die CA regelmäßig neu ausstellt.

7.3.2 OCSP Erweiterungen

Entfällt.

8. Überprüfungen und andere Bewertungen

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

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

Bei Neuaufnahme eines Mitglieds soll diese Überprüfung initial spätestens 3 Monate nach der Aufnahme durchgeführt werden. Bei Bestandmitgliedern wählt der Betreiber mit geeignetem zeitlichem Vorlauf vor Erstellung des Jahresberichts mindestens zwei (innerhalb von 3 Jahren, sollen alle Teilnehmer einmal geprüft worden sein) Mitglieder der Rundfunk-CA zufällig aus und unterzieht diese einer gesonderten Prüfung.

Die Ergebnisse dieser Überprüfung finden Eingang in den Jahresbericht.

Daneben finden ggf. interne Überprüfungen der **RfA Issuing-CA** nach den Maßgaben der Kapitel 8.1 bis 8.6 statt.

8.1 Häufigkeit und Bedingungen für Überprüfungen

Im Fall eines begründeten Verdachts auf Missbrauch der **RfA Issuing-CA** wird von den CA-Administratoren unter Einbindung des IT-Sicherheitsbeauftragten der **RfA** eine anlassbezogene Auswertung der Log-Daten vorgenommen. Es finden keine darüber hinaus gehenden routinemäßigen Kontrollen der Log-Daten statt.

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

8.2 Identität/Qualifikation des Prüfers

Der Prüfer verfügt über eine geeignete Qualifikation als Auditor.

8.3 Stellung des Prüfers zum Bewertungsgegenstand

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

8.4 Durch Überprüfungen abgedeckte Themen

Bei der Konformitätsprüfung der CA werden mindestens folgende Bereiche stichprobenhaft untersucht:

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

8.5 Reaktionen auf Unzulänglichkeiten

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

8.6 Information über Bewertungsergebnisse

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

9. Andere finanzielle und rechtliche Angelegenheiten

9.1 Preise

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

9.1.1 Preise für Zertifikate oder Zertifikatserneuerungen

Entfällt.

9.1.2 Preise für den Zugriff auf Zertifikate

Entfällt.

9.1.3 Preise für Sperrungen oder Statusinformationen

Entfällt.

9.1.4 Preise für andere Dienstleistungen

Entfällt.

9.1.5 Richtlinien für Rückerstattungen

Entfällt.

9.2 Finanzielle Zuständigkeiten

Finanzielle Aspekte werden in diesem Dokument nicht beschrieben.

9.2.1 Versicherungsdeckung

Entfällt.

9.2.2 Andere Posten

Entfällt.

9.2.3 Versicherung oder Gewährleistung für Endnutzer

Entfällt.

9.3 Vertraulichkeitsgrad von Geschäftsdaten

9.3.1 Definition von vertraulichen Informationen

Jegliche Informationen über Teilnehmer und Antragsteller, die nicht unter den nächsten Abschnitt (Kapitel 9.3.2) fallen, werden als vertrauliche Informationen eingestuft und nach den entsprechenden Vorgaben **der RfA** behandelt.

9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören

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

9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen

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

9.4 Datenschutz von Personendaten

9.4.1 Datenschutzkonzept

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

9.4.2 Als persönlich behandelte Daten

Für personenbezogene Daten gelten die Regelungen 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

Soweit dies zur Leistungserbringung der **RFA Issuing-CA(s)** erforderlich ist, erfolgt die Verarbeitung personenbezogener Daten auf einer Rechtsgrundlage nach DSGVO Art. 6 Abs. (1), bspw. zur Erfüllung eines Vertrags (Art. 6 Abs. (1) Lit. b)) oder einer Einwilligung (Art. 6 Abs. (1) Lit. a)) .

Darüber hinaus können alle Informationen veröffentlicht werden, die als nicht vertraulich behandelt werden (siehe Abschnitt 9.4.3) und deren Veröffentlichung nicht widersprochen wurde.

9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften

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

9.4.7 Andere Bedingungen für Auskünfte

Es gibt keine anderen Bedingungen für Auskünfte.

9.5 Geistiges Eigentumsrecht

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

9.6 Zusicherungen und Garantien

9.6.1 Zusicherungen und Garantien der CA

Die **RfA-Issuing-CA** verpflichtet sich, die Anforderungen aus der anwendbaren CP der **RfA-CA** geeignet umzusetzen und alle im Rahmen dieses CPS beschriebenen Aufgaben nach bestem Wissen und Gewissen durchzuführen.

9.6.2 Zusicherungen und Garantien der RA

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

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, ist der beauftragte Dienstleister zur Einhaltung der anwendbaren CP der **RfA-CA** und dieses CPS verpflichtet.

9.7 Haftungsausschlüsse

Entfällt.

9.8 Haftungsbeschränkungen

Entfällt.

9.9 Schadensersatz

Entfällt.

9.10 Gültigkeitsdauer und Beendigung

9.10.1 Gültigkeitsdauer

Dieses Policy-Dokument tritt nach Veröffentlichung in Kraft.

9.10.2 Beendigung

Dieses Policy-Dokument ist solange gültig, bis es durch eine neue Version ersetzt wird oder der Betrieb aller in Kapitel 1.3.1 genannten **RfA-Issuing-CAs** eingestellt wird.

9.10.3 Auswirkung der Beendigung und Weiterbestehen

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

9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern

Andere als die in diesem CPS festgelegten Benachrichtigungen bleiben den CAs freigestellt.

9.12 Ergänzungen

9.12.1 Verfahren für Ergänzungen

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

9.12.2 Benachrichtigungsmechanismen und –fristen

Bei Änderung von Anforderungen im Policy-Dokument der **RfA-Issuing-CA**, die die Endanwender betreffen, werden die Endanwender innerhalb eines Monats durch die **RfA-Issuing-CA** informiert.

9.12.3 Bedingungen für OID Änderungen

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

1.3.6.1.4.1.42638.1.4	**RfA**
1.3.6.1.4.1.42638.1.4.1	CP Dokument der **RfA-CA**
1.3.6.1.4.1.42638.1.4.1.[n]	Hauptversionsnummer
1.3.6.1.4.1.42638.1.4.1.[n].[m]	Nebenversionsnummer
1.3.6.1.4.1.42638.1.4.2	CPS Dokument der **RfA-CA**
1.3.6.1.4.1.42638.1.4.2.[n]	Hauptversionsnummer

1.3.6.1.4.1.42638.1.4.2.[n].[m]	Nebenversionsnummer
1.3.6.1.4.1.42638.1.4.3	erstes CPS Dokument einer **RfA Issuing-CA**
1.3.6.1.4.1.42638.1.4.3.[n]	Hauptversionsnummer
1.3.6.1.4.1.42638.1.4.3.[n].[m]	Nebenversionsnummer
1.3.6.1.4.1.42638.1.4.4	zweites CPS Dokument einer **RfA Issuing-CA**
1.3.6.1.4.1.42638.1.4.4.[n]	Hauptversionsnummer
1.3.6.1.4.1.42638.1.4.4.[n].[m]	Nebenversionsnummer

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

Der OID zur Identifikation des CP-Dokuments der **RfA-CA** und der OID des CPS-Dokuments der **RfA Issuing-CA**, die zum Zeitpunkt der Ausstellung gültig waren, sind in einer Certificate Polices Erweiterung der ausgestellten Zertifikate für **RfA Issuing-CAs** enthalten.

9.13 Verfahren zur Schlichtung von Streitfällen

Grundsätzlich sind die in Abschnitt 1.5.2 genannten Stellen für die Konfliktbeilegung zuständig.

9.14 Zugrundeliegendes Recht

Der Betrieb der **RfA Issuing-CA(s)** unterliegt den Gesetzen der Bundesrepublik Deutschland.

9.15 Einhaltung geltenden Rechts

Die **RfA-Issuing-CA** ist kein Vertrauensdiensteanbieter im Sinne des deutschen Vertrauensdienstegesetzes bzw. der europäischen eIDAS-Verordnung und stellt keine qualifizierten Zertifikate aus. Es werden allenfalls Zertifikate ausgestellt, mit denen fortgeschrittene elektronische Signaturen 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

Entfällt.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses CPS unwirksam sein, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Anstelle der unwirksamen Bestimmungen gilt diejenige wirksame Bestimmung als vereinbart, welche dem Sinn und Zweck der unwirksamen Bestimmung weitgehend entspricht. Im Falle von Lücken gilt ebenfalls dasjenige als vereinbart, was nach Sinn und Zweck dieses CPS vernünftigerweise vereinbart worden wäre, hätte man die Angelegenheit von vorn herein bedacht.

9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

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

9.16.5 Höhere Gewalt

Entfällt.

9.17 Andere Bestimmungen

Entfällt.

10. Anhang

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

10.1 Kontaktdaten

Betreiber der **RfA-Issuing-CA**	Bereich IT-Basis und Infrastruktur des BR (In Personalunion mit den Betreibern der BR-CA)
Vertreter in der CA-Steuerungsgruppe	Lachermeier, Franz - 089-5900-94100, Franz.Lachermeier@br.de
CA-Ansprechpartner für Rundfunk-Root-CA	Tyroller, Thomas - 089-5900-94125, Thomas.Tyroller@br.de Stöcker, Stefan - 089-5900-94133, Stefan.Stoecker@br.de
Certificate Manager der **RfA-Issuing-CA**	Sebastian Beinhofer - Sebastian.Beinhofer@br.de Reinhold Krinninger - Reinhold.Krinninger@br.de
Zuständigkeit für dieses Policy-Dokument	siehe CA-Ansprechpartner
Kontakt für dieses Policy-Dokument	siehe CA-Ansprechpartner
Pflege dieses Policy-Dokuments	siehe CA-Ansprechpartner

Zuständig für die Anerkennung des CP/CPS-Dokuments einer **RfA** Sub-CA	siehe CA-Ansprechpartner

10.2 Zusätzliche Vereinbarungen

10.2.1 Wildcard-Zertifikate

Name (Domain)	Verwendungszweck/Begründung	Ausstellungsdatum	Ablaufdatum
	noch keine erstellt		