Westdeutscher Rundfunk

WDR Sub-CA 01

Zertifizierungsrichtlinie und Regelungen für den Zertifizierungsbetrieb (CP/CPS)

Version 1.1
Datum 06. Juli 2018

Westdeutscher Rundfunk
Appellhofplatz 1
D-50667 Köln

www.wdr.de

Inhaltsverzeichnis

1 Einführung

1.1 Überblick

Der Westdeutsche Rundfunk (im Folgenden kurz: WDR) betreibt eine eigene Public Key Infrastruktur (PKI). Die oberste Instanz der WDR-PKI – die WDR RfA-CA[1] – ist von der Rundfunk-Root-CA zertifiziert. So ist die gesamte WDR PKI Teil der übergreifenden PKI des ARD-Daten-CN der Rundfunkanstalten (siehe Schaubild Abbildung 1). Das ermöglicht gemeinsame PKI-Anwendungen über die Grenzen einzelner Rundfunkanstalten hinweg. Hierzu zählen beim WDR interne SSL/TLS Serverzertifikate[2] und WLAN Client-Authentifikationszertifikate für den WLAN-Zugang beim WDR und anderen Rundfunkanstalten.

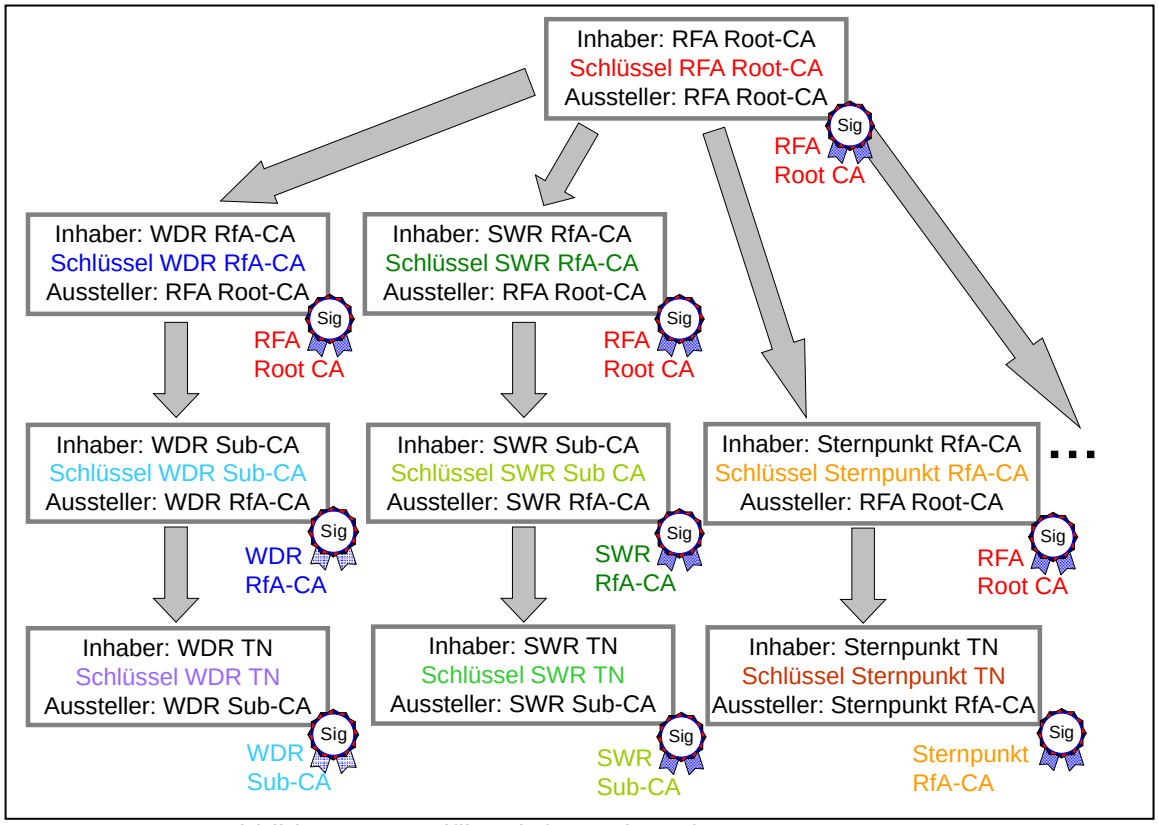

Abbildung 1: Zertifikatsinfrastruktur des ARD-Daten-CN

Dieses Dokument ist eine Kombination der Certificate Policy (CP) und des Certificate Practice Statement (CPS) der WDR Sub-CA 01. Es beschreibt den Zertifizierungsbetrieb der WDR Sub-CA 01 sowie die Anforderungen an Endanwender und Systeme und stellt dar, wie die WDR Sub-CA 01 die Anforderungen der WDR RfA-CA erfüllt.

Alle in diesem Dokument genannten Anforderungen sind für Endanwender (Benutzer, Server und Maschinen bzw. hierfür autorisierte Personen) verbindlich und können nicht abgeschwächt werden.

---

1 Eine RfA-CA ist eine CA, die entweder bei einer Rundfunkanstalt oder einem Dritten für eine Rundfunkanstalt betrieben wird. Sie hängt direkt unter der Rundfunk-Root-CA und kann sowohl Sub-CA-Zertifikate als auch Endanwenderzertifikate ausstellen.

2 WDR-interne Server oder über das ARD Daten-CN erreichbare Server

1.2 Name und Kennzeichnung des Dokuments

Name: Zertifizierungsrichtlinie und Regelungen für den Zertifizierungsbetrieb (CP/CPS) der WDR Sub-CA 01
WDR_Sub-CA_01_CP-CPS_Version_1_1

Version: 1.1

Datum: 06.07.2018

Überarbeitet: Hatice Tuncay, Andreas Hankel

1.3 Teilnehmer der Zertifizierungsinfrastruktur (PKI)

1.3.1 Zertifizierungsstellen

Der WDR betreibt zwei Zertifizierungsstellen: die WDR RfA-CA und die WDR Sub-CA 01. Gegenstand dieser Policy ist die WDR Sub-CA 01.

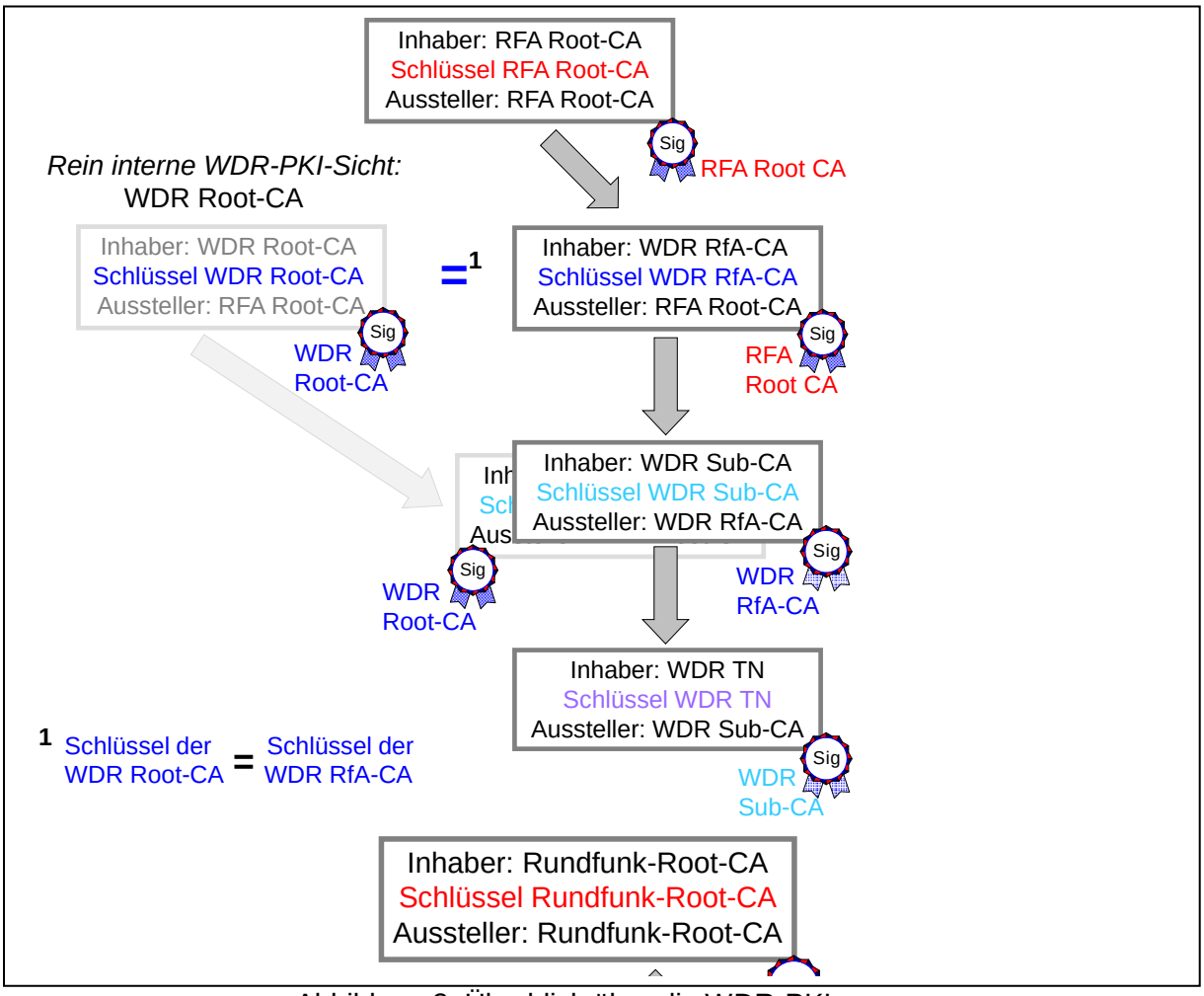

Abbildung 2: Überblick über die WDR-PKI

In Abbildung 2 ist die dreistufige Zertifikatsinfrastruktur-Hierarchie dargestellt, die beim WDR aufgebaut wurde:

- Den Vertrauensanker der Zertifikatsinfrastruktur bildet die Rundfunk-Root-CA.
- Die Rundfunk-Root-CA zertifiziert die WDR RfA-CA. Aus WDR interner PKI-Sicht wird diese WDR RfA-CA auch als Root-CA bezeichnet.

- Die WDR RfA-CA zertifiziert die WDR Sub-CA 01 und ggf. zukünftig weitere Sub-CAs.
- Die WDR Sub-CA 01 stellt Endanwenderzertifikate, speziell SSL/TLS Serverzertifikate und Client-Authentifikationszertifikate für WLAN aus.

1.3.2 Registrierungsstellen

.

Die WDR Sub-CA 01 nutzt die WDR-RA , die Bestandteil der WDR RfA-CA ist.

1.3.3 Zertifikatsinhaber

Zertifikatsinhaber werden im Folgenden auch als Zertifikatsnehmer bezeichnet. Derzeit stellt die WDR Sub-CA 01 nur Authentifikationszertifikate für technische Systeme aus, d.h. für Server, Maschinen und mobile Geräte. Diese Authentifikationszertifikate sind einerseits SSL/TLS-Serverzertifikate und andererseits Client-Authentifikationszertifikate für den WLAN-Zugang beim WDR und anderen Rundfunkanstalten.

1.3.4 Zertifikatsprüfer

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

1.3.5 Weitere Teilnehmer

Die WDR Sub-CA 01 hat technische Ansprechpartner zur Verfügung. Aktuelle Ansprechpartner sind: Peter Ladwig, Andreas Beer

Ansprechpartner der CA-Steuerungsgruppe: Rainer Birkendorf

1.4 Anwendungsbereich

1.4.1 Geeignete Zertifikatsnutzung

Die WDR Sub-CA 01 stellt nur Endanwenderzertifikate für Clients und Server aus. Die zu diesen Zertifikaten gehörenden privaten Schlüssel dürfen nur zur Authentisierung verwendet werden. Diese erlaubte Verwendung wird in den Zertifikaten mittels der Zertifikats-erweiterung *KeyUsage* gekennzeichnet.

Die WDR Sub-CA 01 stellt folgende Endanwenderzertifikate aus:

- SSL/TLS-Serverzertifikate
- Client-Authentifikationszertifikate für den WLAN- Zugang beim WDR und anderen Rundfunkanstalten
- Domain Controller Zertifikate
- OCSP Responder Zertifikate zum Signieren von OCSP Statusauskünften

1.4.2 Untersagte Zertifikatsnutzung

Die WDR Sub-CA 01 stellt keine weiteren Sub-CA-Zertifikate aus. Sie nutzt ihren CA-Schlüssel ausschließlich zur Ausstellung von Endanwenderzertifikaten und Sperrlisten. Sie setzt den CA-Schlüssel nicht für andere Signaturen oder zu Verschlüsselungs- oder Authentisierungszwecken ein.

1.5 Verwaltung und Verantwortung der Zertifizierungsrichtlinie

1.5.1 Zuständigkeit für Zertifizierungsrichtlinie

Zuständig für die Zertifizierungsrichtlinie ist der Betreiber der WDR Sub-CA 01 als Inhaber dieses kombinierten CP/CPS-Dokuments.

1.5.2 Ansprechpartner/Kontaktperson

Die Kontaktperson für die WDR RfA-CA ist der Antragsteller, der das Zertifikat der WDR Sub-CA 01 beim Betreiber der WDR RfA-CA beantragt hat.

Die Kontaktperson für die Endanwender ist der WDR Helpdesk.

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

Diese Zertifizierungsrichtlinie wird einmal im Jahr vom Betreiber der WDR Sub-CA 01 auf Aktualität überprüft.

Die WDR Sub-CA 01 und ihre Einsatzumgebung werden analog zu anderen Windows Serversystemen der WDR IT-Infrastruktur auditiert (siehe Kapitel 8).

1.5.4 Verfahren zur Anerkennung von Regelungen für den Zertifizierungsbetrieb (CPS)

Die WDR Sub-CA 01 erkennt das CP/CPS Dokument der WDR RfA-CA an. Die Umsetzung der Mindestanforderungen dieser Zertifizierungsrichtlinie wird eingehalten. Diese Mindestanforderungen werden nicht abgeschwächt.

1.6 Begriffe und Abkürzungen

AD	**Active Directory** Windows Verzeichnisdienst
AD CS	**Active Directory Certificate Services** Windows CA
C	**Country** Namensattribut für Inhaber- bzw. Aussteller von Zertifikaten
CA	**Certification Authority** Zertifizierungsstelle
CC	**Common Criteria** Internationaler Standard, der die Kriterien für die Bewertung und Zertifizierung der Sicherheit von Computersystemen beschreibt
CIMC	**Certificate Issuing and Management Components** Titel eines Protection Profils, das Anforderungen an Produkte stellt, die Zertifikate erstellen und verwalten
CN	**Common Name** Namensattribut für Inhaber- bzw. Aussteller von Zertifikaten
CN	**Corporate Network**
CP	**Certificate Policy** Zertifizierungsrichtlinie
CPS	**Certification Practice Statement** Regelungen für den Zertifizierungsbetrieb

CRL	**Certificate Revocation List** Sperrliste
CSR	**Certificate Signing Request** Zertifikatsantrag
DN	**Distinguished Name** Vollqualifizierter Name
DNS	**Domain Name System** Namensauflösung im Internet
FIPS	**Federal Information Processing Standard** Amerikanischer Standard für Informationsverarbeitung
HSM	**Hardware Security Modul** Gerät zur sicheren Speicherung und Nutzung kryptographischer Schlüssel
HTTPS	**Hypertext Transfer Protocol Secure** Sicheres Hypertext-Übertragungsprotokoll
IP	**Internet Protocol**
MDM	**Mobile Device Management** System zur zentralen Verwaltung von Mobilgeräten
NIST	**National Institute of Standards and Technology** Bundesbehörde der Vereinigten Staaten
O	**Organization** Namensattribut für Inhaber- bzw. Aussteller von Zertifikaten
OCSP	**Online Certificate Status Protocol** Online-Auskunftsdienst zum Status von Zertifikaten
OID	**Object Identifier** Eindeutiger Kennzeichner für Objekte
PCI	**Payment Card Industry**
PIN	**Personal Identification Number**
PKI	**Public Key Infrastructure** Infrastruktur für X.509 Zertifikate
RA	**Registrierungsstelle**
RDP	**Remote Desktop Protocol**
RfA	**Rundfunkanstalt**
RfA-CA	**Certification Authority einer Rundfunkanstalt** Sub-CA der Rundfunk-Root-CA
SSL/TLS	**Secure Socket Layer / Transport Layer Security**
TPM	**Trusted Platform Module** Spezieller Chip auf einem Gerät als Aufbewahrungsort von kryptographischen Schlüsseln. Das Host-System kann diese zur Authentifizierung nutzen.

UPN	**User Principal Name** Eindeutiges Benennungsschema von Benutzer- und Computerobjekten im AD
VM	**Virtuelle Maschine**
WDR	**Westdeutscher Rundfunk**
WLAN	**Wireless Local Area Network**

2 Veröffentlichungen und Verzeichnisdienst

Die WDR Sub-CA 01 stellt den Zertifikatsnutzern Sperrinformationen über Sperrlisten und über einen OCSP-Responder sowie das eigene von der WDR RfA-CA ausgestellte WDR Sub-CA 01 Zertifikat im AD, im Daten-CN und im Internet[3] zur Verfügung. Dabei stellt der Betreiber der WDR Sub-CA 01 sicher, dass die Veröffentlichung personenbezogener Daten nicht den geltenden Datenschutzrichtlinien widerspricht.

2.1 Verzeichnisdienste

Die komplette Zertifikatskette bestehend aus dem Root-CA Zertifikat der Rundfunk-Root-CA, dem WDR RfA-CA Zertifikat und dem WDR Sub-CA 01 Zertifikat sind im AD des WDR veröffentlicht und können von dort aus dem internen Netz per LDAP abgerufen werden. Im AD stehen auch die Sperrlisten der WDR RfA-CA und der WDR Sub-CA 01 zum Abruf bereit.

Damit Systeme anderer Rundfunkanstalten ggf. die von der WDR Sub-CA 01 erstellten Endanwenderzertifikate prüfen können, wie bspw. WLAN-Zertifikate oder SSL/TLS Serverzertifikate, sind das WDR RfA-CA-Zertifikat, das WDR Sub-CA 01 Zertifikat und Sperrlisten der beiden CAs auch im Daten-CN unter http://wdrmspki.wdr.cn.ard.de veröffentlicht.

WDR-eigene Anwendungen, die nicht auf das AD zugreifen können, z. B. RADIUS Server oder Browser auf Nicht-Windows-Computern, greifen ebenfalls auf die CA-Zertifikate und Sperrlisten im Daten-CN zu.

Um externen Zertifikatsnutzern das WDR RfA-CA Zertifikat, das WDR Sub-CA 01 Zertifikat sowie die Sperrlisten zur Verfügung zu stellen, werden das WDR RfA-CA-Zertifikat, das WDR Sub-CA 01 Zertifikat und die Sperrlisten der beiden CAs zusätzlich im Internet unter http://wdrmspki.wdr.de/ zur Verfügung gestellt.

Die WDR Sub-CA 01 betreibt einen OCSP-Responder, der aus dem WDR-LAN, dem Daten-CN und dem Internet unter den folgenden URLs erreichbar ist:
http://wdrocsp.wdr.de/ocsp

Die URLs für alle oben genannten Abrufmöglichkeiten des WDR Sub-CA 01 Zertifikats und der Sperrliste sowie die URL für den Zugriff auf den OCSP-Responder werden von der WDR Sub-CA 01 in die ausgestellten Endteilnehmerzertifikate eingetragen. So stellt die WDR Sub-CA 01 all ihren Zertifikatsnutzern in geeigneter Weise ihre Sperrinformationen und ihr CA-Zertifikat zur Verfügung.

---

[3] Evtl. soll die WDR Sub-CA 01 zukünftig auch für die Ausstellung von E-Mail-Zertifikaten für das beim WDR betriebene Secure E-Mail Gateway genutzt werden. Da E-Mail-Zertifikate nicht nur WDR-intern, sondern auch von Externen überprüfbar sein müssen, müssen in diesem Fall die CA-Zertifikate der Zertifikatskette und Sperrinformationen auch im Internet verfügbar gemacht werden.

Die URLs für die Abrufmöglichkeiten des WDR RfA-CA Zertifikats und ihrer Sperrliste stehen im CA-Zertifikat der WDR Sub-CA 01.

2.2 Veröffentlichung von Zertifizierungsinformationen

Die Veröffentlichung des WDR Sub-CA 01 Zertifikats im AD, im Daten-CN und im Internet wird einmalig nach der Installation der WDR Sub-CA 01 ausgeführt.

Die Veröffentlichung der Sperrliste im AD, Daten-CN und im Internet erfolgt nach jeder Ausstellung einer neuen Sperrliste durch die WDR Sub-CA 01.

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

Die Sperrliste der WDR Sub-CA ist einen Tag gültig, zuzüglich einer Karenzzeit (für die Behebung eventueller Probleme) von zwei Stunden. Die Sperrliste wird täglich neu ausgestellt.

Die Antwort eines OCSP-Responders zum Status eines Zertifikats ist genauso lange gültig wie der Sperrliste selbst, d. h. einen Tag.

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

2.4 Zugangskontrolle zu Verzeichnisdiensten

Der lesende Zugriff auf die im Abschnitt 2.2 genannten Informationen ist ohne vorherige Anmeldung möglich. Der schreibende Zugriff ist auf berechtigte Personen beschränkt.

3 Identifizierung und Authentifizierung

3.1 Namen

3.1.1 Namensformen

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

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

3.1.2 Aussagekraft von Namen

Die verwendeten Namen sind aussagekräftig und identifizieren den Zertifikatsnehmer eindeutig.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsnehmer

Die von der WDR Sub-CA 01 ausgestellten Endanwenderzertifikate enthalten den Namen des Zertifikatsnehmers (Server oder Maschine) und als Organisation den Westdeutschen Rundfunk.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

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

3.1.5 Eindeutigkeit von Namen

Bei der Ausstellung von Endanwenderzertifikaten stellt die WDR Sub-CA 01 sicher, dass der Distinguished Name des Zertifikatsnehmers innerhalb der WDR Sub-CA 01 eindeutig ist.

3.1.6 Anerkennung, Authentifizierung und Funktion von Warenzeichen

In Endanwenderzertifikaten der WDR Sub-CA 01 werden keine Namen verwendet, die Warenzeichen oder Markennamen verletzen. Markennamen werden anerkannt.

3.2 Identitätsüberprüfung bei Neuantrag

3.2.1 Nachweis des Besitzes des privaten Schlüssels

Die WDR Sub-CA 01 erzeugt selbst keine Schlüssel für Endanwender, aber sie stellt vor der Zertifizierung des öffentlichen Schlüssels sicher, dass der zugehörige private Schlüssel im Besitz des antragstellenden Endanwenders ist.

Die Schlüssel werden von den Endanwendern (Benutzer oder Maschine) oder einer autorisierten Person[4] erzeugt. Im Rahmen eines sicheren Zertifikats- und Schlüsselmanagement-Protokolls wird ein Zertifikatsantrag (CSR) mit eben diesem privaten Schlüssel digital signiert und an die WDR Sub-CA 01 übermittelt.

3.2.2 Authentifizierung von Organisationszugehörigkeiten

Client-Authentifikationszertifikate für Windows Maschinen werden automatisch von den Maschinen, die im AD stehen, beantragt. Client-Authentifikationszertifikate für iPhones werden entweder über ein MDM oder manuell von einem WDR Mitarbeiter als Besitzer des iPhones beantragt. In Ausnahmefällen darf das Client-Authentifikationszertifikate für iPhones auch von dem zuständigen iPhone-Administrator bzw. seinem Vertreter beantragt werden.

SSL/TLS-Serverzertifikate werden stellvertretend von einem WDR-Mitarbeiter beantragt.

Eine gesonderte Prüfung der Organisationszugehörigkeit ist nicht erforderlich, da die Authentifizierung von Organisationszugehörigkeit des Antragstellers auf Basis bereits erfasster Daten erfolgt. Alle berechtigten Antragsteller sind in entsprechenden AD-Gruppen des WDR enthalten.

3.2.3 Anforderungen zur Authentifizierung des Zertifikatsnehmers

Die Authentifizierung des Antragstellers erfolgt auf Basis bereits erfasster Daten. Alle Antragsteller sind im AD des WDR enthalten und authentifizieren sich bei der Windows-Anmeldung mit ihrem AD-Benutzernamen und –Passwort. Auch bei Beantragung eines Client-Authentifikationszertifikats für iPhones über das MDM authentifiziert sich der WDR Mitarbeiter initial über seinen AD-Benutzernamen und Passwort. Daher ist keine weitere Authentifizierung des Antragstellers erforderlich.

Zertifikate für Domain Controller Zertifikate und OCSP-Responder werden automatisch beantragt. Es findet keine Identitätsüberprüfung und Authentifizierung des Antragstellers statt.

3.2.4 Nicht überprüfte Teilnehmerangaben

Es gibt keine nicht geprüften Teilnehmerangaben.

---

4 Autorisiert sind die zuständigen Administratoren für SSL/TLS Server oder iPhones.

3.2.5 Überprüfung der Berechtigung

Client-Authentifikationszertifikate dürfen nur von WDR gemanagten Maschinen im AD, von den zuständigen Administratoren und seinem Vertreter beantragt werden.

Der WDR Sub-CA 01 Admin (siehe Rollenbeschreibung in Abschnitt 5.2.1) vergibt die entsprechenden Antragsberechtigungen in der WDR Sub-CA 01. Zur Berechtigungsverwaltung verwendet der WDR Sub-CA 01 Admin bestehende AD-Gruppen, die von den AD-Administratoren beim WDR gepflegt werden, d.h. nur berechtigte Nutzer können einen Zertifikatsantrag bei der WDR Sub-CA 01 stellen.

SSL/TLS Serverzertifikate können von jedem authentifizierten Benutzer beantragt werden. Die Überprüfung der Antragsberechtigung erfolgt organisatorisch.

3.2.6 Kriterien für Zusammenarbeit

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

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Da bei einem Neuantrag keine gesonderte Identitätsprüfung und Authentifizierung des Antragstellers erforderlich ist, ist diese auch bei einer Zertifikatserneuerung nicht erforderlich.

3.3.2 Zertifikatserneuerung nach einer Sperrung

Da bei einem Neuantrag keine gesonderte Identitätsprüfung und Authentifizierung des Antragstellers erforderlich ist, ist diese auch bei Anträgen zur Zertifizierung nach einer Sperrung nicht erforderlich.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Sperranträge für alle Client-Authentifizierungszertifikate werden vom WDR Mitarbeiter über den Arbeitsplatz-Service oder das Helpdesk gestellt. Diese tragen den Sperrantrag im WDR Ticket-System ein. Hierfür muss sich der Mitarbeiter vom Arbeitsplatz-Service bzw. Helpdesk am Ticket-System authentifizieren.

Die Sperrung eines SSL-Serverzertifikats wird von dem Server-Administrator oder seinem Vertreter direkt beim WDR Sub-CA 01 Manager (siehe Rollenbeschreibung in Abschnitt 5.2.1) beantragt. Die Identitätsprüfung und Authentifizierung des Antragstellers erfolgt organisatorisch. Bei Gefahr in Verzug ist zusätzlich zum Server-Administrator und seinem Vertreter auch das Netzwerk-Security-Betriebsteam sperrberechtigt. In Ausnahmefällen. z. B. bei Missbrauch oder Nicht-Einhaltung der Sicherheitsanforderungen durch den Server-Administrator oder seinen Vertreter ist zusätzlich auch das IT-Sicherheitsteam sperrberechtigt. Die Mitarbeiter des Netzwerk-Security-Betriebsteams und des IT-Sicherheitsteams sind dem WDR Sub-CA 01 Manager persönlich bekannt. Daher ist in diesen Fällen keine gesonderte Identitätsprüfung und Authentifizierung des Antragstellers erforderlich.

4 Ablauforganisation

4.1 Zertifikatsantrag

4.1.1 Wer kann ein Zertifikat beantragen

Derzeit stellt die WDR Sub-CA 01 Authentisierungszertifikate für technische Systeme (Server und Clients) des WDR und Zertifikate für ihren OCSP-Responder aus. Client-Authentifizierungszertifikate werden entweder durch eine WDR-eigene Maschine im AD, von einem WDR Mitarbeiter oder bei iPhones von dem zuständigen iPhone-Administrator bzw. seinem Vertreter beantragt. SSL/TLS Serverzertifikate können von jedem authentifizierten Benutzer beantragt werden. Die Überprüfung der Antragsberechtigung erfolgt organisatorisch.

4.1.2 Verfahren und Zuständigkeiten

Die Client-Authentifikationszertifikate für Windows-Maschinen werden automatisch bei der WDR Sub-CA 01 beantragt. Andere Client-Authentifikationszertifikate wie bspw. für iPhones werden entweder über ein MDM oder manuell von dem WDR Mitarbeiter als Besitzer des iPhones bzw. stellvertretend von einem iPhone-Administrator bei der WDR Sub-CA 01 beantragt.

Anträge für SSL/TLS-Serverzertifikate werden manuell von einem authentifizierten Benutzer über eine Web-Schnittstelle bei der WDR Sub-CA 01 eingereicht. Vor Ausstellung des SSL-Serverzertifikats prüft der WDR Sub-CA 01 Manager den Zertifikatsantrag.

Bei OCSP-Responder-Zertifikaten wird vom OCSP-Responder ein Schlüsselpaar erzeugt und ein entsprechender Zertifizierungsantrag (CSR) bei der WDR Sub-CA 01 eingereicht.

4.2 Bearbeitung von Zertifikatsanträgen

4.2.1 Durchführung von Identifikation und Authentifizierung

Bei der Bearbeitung von Zertifikatsanträgen sind keine gesonderte Identitätsprüfung und Authentifizierung des Antragstellers erforderlich, da die Authentifizierung des Antragstellers schon im vorangegangenen Schritt bei der Zertifikatsbeantragung durchgeführt wurde. Die Authentifizierung des Antragstellers erfolgt auf Basis bereits erfasster Daten im AD des WDR. Jede neu generierte WDR Sub-CA wird im Ticketsystem dokumentiert.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Alle Client-Authentifikationszertifikate werden von der WDR Sub-CA 01 automatisch ausgestellt, sofern sie syntaktisch korrekt sind. Lediglich Zertifikatsanträge für SSL/TLS-Serverzertifikate werden von dem WDR Sub-CA 01 Manager manuell auf die Namensgebung im Zertifikatsantrag geprüft und in Abhängigkeit dieser Prüfung über Annahme oder Ablehnung des Antrags entschieden.

4.2.3 Bearbeitungsdauer bei Zertifikatsanträgen

Alle Client-Authentifikationszertifikate werden umgehend ausgestellt.

Die Ausstellung von SSL/TLS-Serverzertifikaten erfolgt innerhalb von 14 Tagen ab Eingang des Antrags über die Web-Schnittstelle, sofern alle zur Beantragung benötigten Dokumente vorliegen.

4.3 Zertifikatserstellung

4.3.1 Aufgaben der Zertifizierungsstelle

Die Ausstellung von Client-Authentifikationszertifikate durch die WDR Sub-CA 01 erfolgt automatisch.

Zertifikatsanträge für SSL/TLS-Serverzertifikate werden über die AD oder die Webseite http://zertifikatsantrag.wdr.de eingereicht. Der Antragssteller ist der angemeldete User am System. Anschließend wird von dem WDR Sub-CA 01 Manager manuell die Namensgebung im Zertifikatsantrag geprüft und erst dann in Abhängigkeit dieser Prüfung zur Ausstellung freigegeben. Das ausgestellte Zertifikat wird entweder automatisch zur Verfügung gestellt oder kann durch den beantragenden User über die Webseite heruntergeladen werden.

4.3.2 Benachrichtigung des Antragstellers

Es findet keine zusätzliche Benachrichtigung bzgl. der Zertifikatserstellung statt.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme des Zertifikats

Es ist kein dedizierter Prozess zur Zertifikatsannahme durch den Endanwender vorgesehen.

4.4.2 Veröffentlichung des Zertifikats durch die Zertifizierungsstelle

Die WDR Sub-CA 01 stellt ihr CA-Zertifikat im AD, im Daten-CN und im Internet zum Abruf bereit.

4.4.3 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Es findet keine Benachrichtigung weiterer Instanzen statt.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Nutzung durch den Zertifikatsnehmer

Die WDR Sub-CA 01 setzt ihren Schlüssel und ihr Zertifikat nur für die in ihrem Zertifikat genannten Verwendungszwecke ein. Sie trägt dafür Sorge, dass ihr privater Schlüssel angemessen geschützt ist (siehe Kapitel 6).

Sollte der private Schlüssel der WDR Sub-CA dennoch abhandengekommen, gestohlen oder möglicherweise kompromittiert worden sein oder sollten Angaben im Zertifikat nicht mehr korrekt sein, wird unverzüglich ein Sperrantrag bei der WDR RfA-CA gestellt.

Die gleiche Anforderung im Umgang mit dem privaten Schlüssel und Zertifikat gilt auch für die Zertifikatsnehmer (Endanwender) der WDR Sub-CA 01: Ein Endanwender darf seinen privaten Schlüssel und sein Zertifikat nur für die im Zertifikat genannten Verwendungszwecke einsetzen. Er bzw. die für den Schlüssel und das Zertifikat autorisierte Person muss dafür Sorge tragen, dass der private Schlüssel angemessen geschützt ist. Er bzw. die autorisierte Person muss das Zertifikat unverzüglich sperren lassen, wenn die Angaben des Zertifikats nicht mehr korrekt sind, oder wenn der private Schlüssel abhandengekommen, gestohlen oder möglicherweise kompromittiert wurde.

4.5.2 Nutzung des Zertifikats durch die Relying Party

Ein Zertifikatsprüfer darf ein Zertifikat nur für die im Zertifikat genannten Verwendungszwecke akzeptieren.

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

4.6.1 Bedingungen für eine Zertifikatserneuerung

Eine Zertifikatserneuerung unter Beibehaltung des alten WDR Sub-CA 01 Schlüssels findet nicht statt. Mit der Erneuerung des WDR Sub-CA 01 Zertifikats werden auch neue Schlüssel erzeugt (siehe Abschnitt 4.7). Im Fall einer Zertifikatserneuerung für einen Endteilnehmer muss in jedem Fall auch zwingend eine Schlüsselerneuerung stattfinden (siehe Abschnitt 4.7).

4.6.2 Wer darf eine Zertifikatserneuerung beantragen

Eine Zertifikatserneuerung unter Beibehaltung des alten WDR Sub-CA 01 Schlüssels findet nicht statt. Es gelten die gleichen Regelungen wie bei einer Neubeantragung und sind im Kapitel 4.3 dokumentiert.

4.6.3 Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung

Eine Zertifikatserneuerung unter Beibehaltung des alten WDR Sub-CA 01 Schlüssels findet nicht statt. Es gelten die gleichen Regelungen wie bei einer Neubeantragung und sind im Kapitel 4.3 dokumentiert.

4.7 Schlüssel- und Zertifikatserneuerung

Bei einer Zertifikatserneuerung mit Schlüsselwechsel wird einem Zertifikatsnehmer (Endanwender), der bereits ein Zertifikat besitzt, durch die WDR Sub-CA 01 ein neues Zertifikat für einen neuen Schlüsselpaar ausgestellt, sofern die im Zertifikat enthaltenen Informationen unverändert bleiben. Der Endanwender erzeugt die neuen Schlüssel selber.

4.7.1 Gründe für eine Schlüssel- und Zertifikatserneuerung

Die WDR Sub-CA 01 führt rechtzeitig, d.h. mindestens drei Jahre vor Ablauf ihres Zertifikats eine Schlüssel- und Zertifikatserneuerung durch[5]. Musste das WDR Sub-CA 01 Zertifikat gesperrt werden, aber ein entsprechendes Zertifikat wird weiterhin benötigt, führt die WDR Sub-CA 01 ebenfalls eine Schlüssel- und Zertifikatserneuerung durch.

Auch für Endanwender gilt: Grund für eine Schlüssel- und Zertifikatserneuerung ist der bevorstehende Ablauf des Zertifikats. Eine Schlüssel- und Zertifikatserneuerung muss auch stattfinden, wenn ein Zertifikat widerrufen wurde, aber ein entsprechendes Zertifikat weiterhin benötigt wird.

4.7.2 Wer kann eine Schlüssel- und Zertifikatserneuerung beantragen

Es gelten die gleichen Regelungen wie bei einer Neubeantragung.

4.7.3 Ablauf der Schlüssel- und Zertifikatserneuerung

Es gelten die gleichen Regelungen wie bei einer Neubeantragung.
Die Schlüssel- und Zertifikatserneuerung bei Client-Authentifikationszertifikaten erfolgt soweit möglich automatisch.

---

5 Endanwenderzertifikate sind maximal drei Jahre gültig. Das Zertifikat der WDR Sub-CA 01 muss zum Zeitpunkt der Ausstellung mindestens noch genau so lange gültig sein.

4.7.4 Benachrichtigung des Zertifikatsnehmers

Mit einer ausreichenden Vorlaufzeit von mindestens sechs Wochen wird für die SSL/TLS-Serverzertifikate an die bei der Zertifikatsbeantragung angegebene Kontakt-E-Mail-Adresse automatisch eine Erinnerungs-Mail versendet, die auf den bevorstehenden Ablauf eines SSL/TLS-Serverzertifikats hinweist.

Solange die Client-Authentifikationszertifikate für iPhones beim WDR manuell beantragt werden, erhalten die iPhone Besitzer ebenso sechs Wochen vor Ablauf des Zertifikats eine Erinnerungs-Mail mit dem Hinweis auf den bevorstehenden Ablauf des Zertifikats und eine ggf. notwendige Erneuerung. Sobald die Client-Authentifikationszertifikate für iPhones über ein MDM verwaltet werden, entfällt diese Erinnerungs-Mail.

Für Client-Authentifikationszertifikate von Windows-Maschinen werden keine Erinnerungs-Mails versendet, da diese automatisch verlängert werden.

4.7.5 Annahme der Schlüssel- und Zertifikatserneuerung

Es gibt keinen dedizierten Prozess zur Annahme der Schlüssel- und Zertifikatserneuerung durch Endanwender.

4.7.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle

Es gelten die gleichen Regelungen wie bei einer Neubeantragung.

4.7.7 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Es findet keine Benachrichtigung weiterer Instanzen statt.

4.8 Zertifikatsänderung

4.8.1 Gründe für eine Zertifikatsänderung

Wenn sich Angaben im Zertifikat der WDR Sub-CA 01 geändert haben, stellt die WDR Sub-CA 01 einen Antrag auf Zertifikatsänderung bei der WDR RfA-CA.

Grund für eine Zertifikatsänderung eines CA-Zertifikats ist zum Beispiel:

- der Name des Zertifikatsnehmers hat sich wegen einer Umstrukturierung der Organisation geändert

Haben sich Angaben in einem Endanwenderzertifikat geändert, so muss der Endanwender eine Zertifikatsänderung bei der WDR Sub-CA 01 beantragen. Gründe für eine Zertifikatsänderung sind zum Beispiel:

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

4.8.2 Wer kann eine Zertifikatsänderung beantragen

Es gelten die gleichen Regelungen wie bei einer Neubeantragung.

4.8.3 Ablauf der Zertifikatsänderung

Eine Zertifikatsänderung bedeutet technisch die Sperrung des alten Zertifikats und eine Schlüssel- und Zertifikatserneuerung. Für den Ablauf gelten die gleichen Regelungen wie in Abschnitt 4.9 und 4.7 beschrieben.

4.8.4 Benachrichtigung des Zertifikatsnehmers

Die Endanwender werden nicht vom WDR Sub-CA 01 Admin bzw. WDR Sub-CA 01 Manager über eine notwendige Zertifikatsänderung benachrichtigt. Verantwortlich für die Beantragung einer Zertifikatsänderung sind die Endanwender selbst.

4.8.5 Annahme der Zertifikatsänderung

Es gibt keinen dedizierten Prozess zur Annahme der Zertifikatsänderung.

4.8.6 Veröffentlichung einer Zertifikatsänderung durch die Zertifizierungsstelle

Es gelten die gleichen Regelungen wie bei einer Neubeantragung.

4.8.7 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Es findet keine Benachrichtigung weiterer Instanzen statt.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Gründe für eine Sperrung

Ein WDR Sub-CA 01 Zertifikat wird widerrufen, wenn mindestens einer der folgenden Fälle eintritt:

- Das Zertifikat enthält Angaben, die nicht gültig sind.
- Der private Schlüssel des Zertifikatsnehmers wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
- Die WDR Sub-CA 01 stellt den Zertifizierungsbetrieb ein.
- Die Endteilnehmer halten Anforderungen aus diesem CP/CPS nicht ein
- Die WDR Sub-CA 01 hält die Regelungen ihres CP/CPS nicht ein; somit sollten auch alle von ihr ausgestellten Endteilnehmerzertifikate gesperrt werden.
- Der Zertifikatsnehmer ist nicht mehr berechtigt, das Zertifikat zu nutzen.
- Der Zertifikatsnehmer benötigt das Zertifikat nicht mehr.

4.9.2 Wer kann eine Sperrung beantragen

Ein WDR Mitarbeiter informiert das Helpdesk, wenn sein Client-Authentifikationszertifikat gesperrt werden muss. Den Sperrantrag für Client-Authentifikationszertifikate von Notebooks und iPhones stellt dann das WDR Helpdesk bei der WDR Sub-CA 01. Auch der Arbeitsplatz-Service ist sperrberechtigt für Client-Authentifikationszertifikate.

Sperrberechtigt für ein SSL/TLS Serverzertifikat ist der Server-Administrator oder sein Vertreter. Bei Gefahr in Verzug ist zusätzlich zum Server-Administrator und seinem Vertreter auch das Netzwerk-Security-Betriebsteam sperrberechtigt. In Ausnahmefällen. z. B. bei Missbrauch oder Nicht-Einhaltung der Mindestanforderungen aus diesem CP/CPS vom Zertifikatsnehmer bzw. der autorisierten Person[4] ist zusätzlich auch das IT-Sicherheitsteam sperrberechtigt.

4.9.3 Ablauf einer Sperrung

Die Sperrung von SSL/TLS-Serverzertifikaten und WLAN-Zertifikaten sowie die Ausstellung einer neuen Sperrliste wird vom WDR Sub-CA 01 Manager durchgeführt. Er fertigt über diesen Vorgang eine schriftliche Protokollnotiz an und archiviert diese in geeigneter Form. Abschließend exportiert er die neue Sperrliste und publiziert diese auf dem Web-Server, im Intranet und Internet. Die Veröffentlichung im AD erfolgt automatisch.

4.9.4 Fristen für den Zertifikatsnehmer

Bei Bekanntwerden eines Sperrgrundes beantragt die WDR Sub-CA 01 umgehend die Sperrung ihres Zertifikats bei der WDR RfA-CA.

Ebenso muss auch bei Bekanntwerden eines Sperrgrundes für ein Client-Authentifikations-zertifikat der WDR Mitarbeiter unverzüglich das Helpdesk informieren. Das Helpdesk muss unverzüglich die Sperrung beantragen. Bei Bekanntwerden eines Sperrgrundes für ein SSL/TLS-Serverzertifikat muss der Server-Administrator oder sein Vertreter unverzüglich die Sperrung beantragen.

4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle

Die Sperrung eines SSL/TLS-Serverzertifikats oder eines Client-Authentifikationszertifikats wird innerhalb eines Arbeitstags vom WDR Sub-CA 01 Manager durchgeführt.

4.9.6 Anforderung zu Sperrprüfungen durch eine Relying Party

Ein Zertifikatsprüfer (Relying Party) muss bei jedem Einsatz die Gültigkeit der Zertifikate überprüfen. Hierzu muss er entweder eine OCSP-Auskunft einholen oder die aktuelle Sperrliste beziehen und diese auf das verwendete Zertifikat prüfen.

4.9.7 Häufigkeit der Sperrlistenveröffentlichung

Die Sperrliste der WDR Sub-CA 01 wird täglich neu ausgestellt. Sie ist einen Tag gültig, zuzüglich einer Karenzzeit von zwei Stunden. Stündlich wird die Liste auch auf dem Webserver aktualisiert. Im Falle einer Sperrung wird eine neue Sperrliste ausgeführt und publiziert.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die maximale Latenzzeit für Sperrlisten der WDR Sub-CA 01 (Zeitpuffer zwischen Erstellung und Veröffentlichung der Sperrlisten) beträgt zwei Stunden.

4.9.9 Verfügbarkeit von Online-Statusabfragen (OCSP)

Die WDR Sub-CA 01 bietet einen Online-Dienst zur Auskunft der Gültigkeit von Zertifikaten an. Die URL dieses Online-Auskunftsdienstes ist in allen Endteilnehmerzertifikaten enthalten. Der Online-Auskunftsdienst ist aus dem internen Netz, dem Daten-CN und dem Internet erreichbar.

4.9.10 Anforderungen an Online-Statusabfragen (OCSP)

Siehe Kapitel 7.3

4.9.11 Andere verfügbare Formen der Widerrufsbekanntmachung

Die WDR Sub-CA 01 macht Widerrufe in keiner anderen Form als über Sperrlisten und OCSP bekannt.

4.9.12 Anforderungen bei Kompromittierung von privaten Schlüsseln

Bei Kompromittierung eines privaten Schlüssels wird das zugehörige Endanwenderzertifikat nach Bekanntwerden der Meldung unverzüglich durch die WDR Sub-CA 01 widerrufen und umgehend –auch außerhalb des regulären Rhythmus– eine neue Sperrliste veröffentlicht.

4.9.13 Gründe für eine Suspendierung

Eine temporäre Sperrung bzw. eine Suspendierung von Zertifikaten findet nicht statt.

4.9.14 Wer kann Suspendierung beantragen

Eine Suspendierung von Zertifikaten findet nicht statt.

4.9.15 Ablauf einer Suspendierung

Eine Suspendierung von Zertifikaten findet nicht statt.

4.9.16 Maximale Sperrdauer bei Suspendierung

Eine Suspendierung von Zertifikaten findet nicht statt.

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

4.10.1 Betriebsbedingte Eigenschaften

Der OCSP-Responder der WDR Sub-CA 01 bezieht seine Sperrinformationen aus der aktuellen Sperrliste der WDR Sub-CA 01.

OCSP-Auskünfte werden mit einem eigenen OCSP-Responder-Signing-Schlüssel unterschrieben. Es ist „Best Practice“, dass OCSP-Signing-Zertifikate nicht gesperrt werden. Daher sind OCSP-Signing- Zertifikate nur für eine kurze Zeit gültig und werden automatisch neu ausgestellt. Die Neuausstellung des Zertifikats ist stets auch mit der Erzeugung von neuem Schlüsselmaterial verbunden.

Da der OCSP-Responder auch vom Internet aus erreichbar sein muss, wird der private Schlüssel des OCSP-Responders in einem HSM gespeichert, so dass er nicht kompromittiert werden kann[6].

4.10.2 Verfügbarkeit des Dienstes

Der Online-Dienst zur Auskunft der Gültigkeit von Zertifikaten muss nicht hoch verfügbar sein, da alternativ der Status eines Endanwenderzertifikats anhand der Sperrliste der WDR Sub-CA 01 geprüft werden kann.

4.10.3 Weitere Merkmale

Keine weiteren Festlegungen.

4.11 Beendigung des Vertragsverhältnisses

Bei Beendigung des Arbeitsvertrags eines WDR Mitarbeiters müssen alle seine Client-Authentifikationszertifikate gesperrt werden.

4.12 Schlüsselhinterlegung und Wiederherstellung

4.12.1 Richtlinien und Verfahren zur Schlüsselhinterlegung und Wiederherstellung

Die WDR Sub-CA 01 bietet keine Schlüsselhinterlegung für Endanwender an.

4.12.2 Richtlinien und Verfahren zum Schutz und Wiederherstellung von Sitzungsschlüsseln

Es werden keine Sitzungsschlüssel verwendet.

---

6 Wäre ein OCSP-Responder-Signing-Schlüssel kompromittiert, könnten OCSP-Auskünfte gefälscht und so von der WDR Sub-CA 01 gesperrte Zertifikate von Zertifikatsprüfern als gültig anerkannt werden.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Alle zentralen Komponenten der WDR Sub-CA 01 sind in einer geschützten Umgebung im Rechenzentrum des WDR untergebracht. Dort werden physikalische Sicherheitsmaßnahmen angewandt, die dem Stand der Technik entsprechen. Der Schutz der PKI-Komponenten entspricht dem anderer Serversysteme, die beim WDR im Einsatz sind.

Zum Schutz des privaten Schlüssels werden sowohl der private Schlüssel der WDR Sub-CA 01 als auch der private Schlüssel des OCSP-Responders in einem HSM erzeugt und gespeichert.

5.2 Organisatorische Sicherheitsmaßnahmen

Alle zentralen Komponenten der WDR Sub-CA 01 werden im Rechenzentrum des Unternehmens durch organisatorische Sicherheitsmaßnahmen geschützt. Der organisatorische Schutz der PKI-Komponenten entspricht dem anderer Serversysteme, die beim WDR im Einsatz sind.

5.2.1 Rollenkonzept

Für den Aufbau und Betrieb der WDR Sub-CA 01 werden folgende Rollen unterschieden:

Rolle	Typ der Rolle	Mindest-Anzahl der Personen	Aufgaben
Enterprise-Administrator	Betriebs-system	1	Installation der WDR Sub-CA 01
Domänen-Administrator der AD-Domäne, in der die WDR Sub-CA 01 installiert wird	Betriebs-system	1	Installation der WDR Sub-CA 01
Lokaler Administrator der WDR Sub-CA 01 (entspricht CIMC Administrator)	Betriebs-system	1	Administration des Betriebssystems der WDR Sub-CA 01 (gleicher Aufwand wie bei anderen Windows Servern) Installation der AD Certificate Services (einmaliger Aufwand) Konfiguration der Rollentrennung gemäß Common Criteria (einmaliger Aufwand bei der Installation der AD CS) Erneuerung des WDR Sub-CA 01 Zertifikats nach 10 Jahren (erfordert Zugriff auf den *Local Machine's Certificate Store*)

WDR Sub-CA 01 Admin (entspricht CIMC Administrator)	PKI	1[7]	Konfiguriert und pflegt die WDR Sub-CA 01. Insbesondere konfiguriert er die Zertifikats-, Sperrlisten- und OCSP-Responder-Profile. Dies ist ein einmaliger Prozess, ggf. fallen Aufwände für nachträgliche Änderungen an.
WDR Sub-CA 01 Manager (entspricht CIMC Officer)	PKI	1[7]	Ist zuständig für Freigabe, Ausstellung und Sperrung von Zertifikaten für Endteilnehmer, siehe Beschreibung der Betriebsprozesse in Kapitel 5
Tresorverwalter für den Tresor im Archivhaus	Schließ-regelung	1	Zugriff auf den Tresor im Archivhaus beim WDR. Dort werden verwahrt: • Versiegelter Passwort-Brief für Partition auf dem erstem HSM mit dem WDR Sub-CA 01 Schlüssel • Versiegelter Passwort-Brief für Partition auf dem zweiten HSM mit dem WDR Sub-CA 01 Schlüssel • Versiegelter Passwort-Brief für Partition auf dem erstem HSM mit dem OCSP-Responder-Schlüssel • Versiegelter Passwort-Brief für Partition auf dem zweiten HSM mit dem OCSP-Responder-Schlüssel • Versiegelter Passwort-Brief mit Pre-Boot-Passwort für Laufwerks-verschlüsselung • Rescue Disk für Laufwerks-verschlüsselung • Versiegelter Passwort-Brief mit dem Passwort des lokalen System Administrators des OCSP-Responders

Tabelle 1: Rollen für Aufbau und Betrieb der WDR Sub-CA 01

5.2.2 Anzahl involvierter Personen pro Aufgabe

Die WDR Sub-CA 01 bietet keine Wiederherstellung von Verschlüsselungsschlüsseln (Key Recovery) an; daher ist kein Vier-Augen-Prinzip erforderlich. Für keine der Rollen beim Aufbau und Betrieb der WDR Sub-CA 01 wird ein Vier-Augen-Prinzip umgesetzt. Jede Rolle wird von einer Person alleine ausgeübt.

5.2.3 Identifizierung und Authentifizierung jeder Rolle

Die Authentifizierung bei allen der oben genannten Rollen ist eine Ein-Faktor-Authentifizierung über Benutzername und Passwort.

5.2.4 Rollen, die eine Aufgabentrennung erfordern

Die für die Systeme beim WDR verantwortlichen Rollen sind personell von den Rollen getrennt, die den PKI-Betrieb leisten, d.h. der Enterprise-, der Domänen-Administrator und

[7] Die Rolle des WDR Sub-CA 01 Admins und des WDR Sub-CA 01 Managers werden von zwei verschiedenen Personen wahrgenommen.

der Lokale Administrator der WDR Sub-CA 01 sind von dem WDR Sub-CA 01 Admin und dem WDR Sub-CA 01 Manager getrennt.

Die Rolle des Tresorverwalters für den Tresor im Archivhaus beim WDR wird in Personalunion vom WDR Sub-CA 01 Admin oder dem WDR Sub-CA 01 Manager übernommen[8].

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an Mitarbeiter

Der WDR Sub-CA 01 Admin und der WDR Sub-CA 01 Manager sind feste Mitarbeiter des WDR. Sie sind zur Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet. Sie verfügen über ausreichende Fachkunde, um die WDR Sub-CA 01 sicher zu betreiben. Sie kennen den Stand der Technik und die Best Practices im Bereich Zertifikatsinfrastrukturen.

Hinsichtlich Fachkunde im Bereich Zertifikatsinfrastrukturen bestehen keine Anforderungen an die Endanwender beim WDR.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Für die WDR Sub-CA 01 Admins und WDR Sub-CA 01 Manager wird keine Sicherheits-überprüfung durchgeführt.

Auch für die Endanwender ist keine Sicherheitsüberprüfung erforderlich.

5.3.3 Anforderungen an Schulungen

Es bestehen keine Anforderungen an Schulungen.

5.3.4 Häufigkeit und Anforderungen an Fortbildungen

Der WDR Sub-CA 01 Admin und der WDR Sub-CA 01 Manager besuchen mindestens alle zwei Jahre eine PKI-Schulung oder halten sich auf andere Weise über den Stand der Technik und die Best Practices im Bereich PKI auf dem Laufenden.

Hinsichtlich Fortbildung im Bereich Zertifikatsinfrastrukturen bestehen keine Anforderungen an die Endanwender beim WDR.

5.3.5 Häufigkeit und Ablauf von Arbeitsplatzwechseln

Es findet kein regelmäßiger Arbeitsplatzwechsel für den WDR Sub-CA 01 Admin und den WDR Sub-CA 01 Manager statt.

5.3.6 Sanktionen für unerlaubte Handlungen

Der WDR Sub-CA 01 Admin und der WDR Sub-CA 01 Manager unterliegen – wie alle Mitarbeiter des WDR - den arbeitsrechtlich zulässigen Sanktionsmöglichkeiten.

5.3.7 Anforderungen an freie Mitarbeiter

Es gibt keine zusätzlichen Anforderungen an freie Mitarbeiter.

---

8 Die Rolle des Tresorverwalters darf nicht in Personalunion mit der Rolle des „Lokaler Administrator der WDR Sub-CA 01“ von der gleichen Person übernommen werden, da die Rescue Disk für die Laufwerksverschlüsselung der WDR Sub-CA 01 dem Lokalen Administrator nicht zugänglich sein darf.

5.3.8 Dokumentation für Mitarbeiter

Der WDR Sub-CA 01 Admin und der WDR Sub-CA 01 Manager erhalten das kombinierte CP/CPS-Dokument der WDR RfA-CA mit seinen Anforderungen an untergeordnete WDR Sub-CAs und dieses Dokument mit der Beschreibung der Umsetzung dieser Anforderungen zur Kenntnis.

Mitarbeitern beim WDR ist eine Kurzanleitung für die Bedienung der jeweiligen PKI-Anwendung und den sicheren Umgang mit ihrem privaten Schlüssel zur Verfügung zu stellen.

5.4 Überwachungsmaßnahmen

Alle sicherheitsrelevanten Ereignisse der WDR Sub-CA 01 werden in Log-Dateien protokolliert. Die AD Certificate Services nutzen das Windows Ereignisprotokoll für ihre Log-Daten.

5.4.1 Überwachte Ereignisse

Zu den sicherheitsrelevanten Ereignisse der WDR Sub-CA 01 zählen z. B.:

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

5.4.2 Häufigkeit der Protokollanalyse

Die WDR Sub-CA ist an das beim WDR bestehende Sysmon-System zur routinemäßigen Überprüfung auf sicherheitsrelevante Einträge im Windows Ereignisprotokoll angeschlossen. So werden die Log-Daten der WDR Sub-CA 01 kontinuierlich auf sicherheitsrelevante Einträge überprüft. Darüber hinaus wird im Fall eines begründeten Verdachts auf Missbrauch der WDR Sub-CA 01 von einem WDR Sub-CA 01 Admin oder WDR Sub-CA 01 Manager eine anlassbezogene Auswertung der Log-Daten der WDR Sub-CA nach Vorgabe der IT-Sicherheitsordnung des WDR vorgenommen.

5.4.3 Aufbewahrungsfrist für Protokolldaten

Das Windows Ereignisprotokoll, das u.a. auch die Protokolldaten der WDR Sub-CA 01 enthält, wird mindestens 6 Monate im Backup-System aufbewahrt.

5.4.4 Schutz von Protokolldaten

Die Protokolldaten der WDR Sub-CA 01 sind über die Zugriffskontrolle des Betriebssystems gegen unberechtigten Zugriff, Löschung und Manipulation geschützt.

5.4.5 Backup der Protokolldaten

Zur Nachvollziehbarkeit von ausgestellten Zertifikaten, gesperrten Zertifikaten und der Ausstellung von Sperrlisten werden die Log-Dateien der WDR Sub-CA 01 regelmäßig gesichert. Hierzu sind sie in das Backup-System beim WDR integriert.

5.4.6 Überwachungssystem

Die WDR Sub-CA 01 ist in die Betriebsüberwachung beim WDR integriert. Als Monitoring-Werkzeuge ist beim WDR das Sysmon-System im Einsatz.

5.4.7 Benachrichtigung bei schwerwiegenden Ereignissen

Keine weiteren Festlegungen. Siehe Kapitel 5.4.2

5.4.8 Schwachstellenanalyse

Die Software der WDR Sub-CA 01 wurde in das Patch-Management des WDR aufgenommen. Schwachstellen in dem eingesetzten System (AD CS) werden nach Bekanntwerden der Schwachstelle und Vorliegen eines Patches umgehend geschlossen.

Auch die PKI-Client- und Server-Software, die Zertifikate der WDR Sub-CA 01 nutzen, sind in das Patch-Management des WDR aufzunehmen. Schwachstellen bei den eingesetzten Systemen sind nach Bekanntwerden der Schwachstelle und Vorliegen eines Patches umgehend zu schließen.

5.5 Archivierung

5.5.1 Archivierte Daten

Art und Umfang der aufzubewahrenden Daten:

- Sicherheitskopie des WDR Sub-CA 01 Schlüssels auf zweiten Ersatz-HSM, das als Hot-Standby bereitsteht
- Passwort-Briefe mit den Partitions-Passwörtern für die beiden HSMs, das Pre-Boot-Passwort sowie die Rescue Disk für die Laufwerksverschlüsselung
- Sperranträge an die WDR Sub-CA 01 (formfreier Antrag bei SSL Serverzertifikaten und Ticket im WDR Ticket-System bei Client-Authentifikationszertifikaten)
- Aktuelles Backup der WDR Sub-CA 01 Zertifikatsdatenbank
- Log-Dateien der WDR Sub-CA 01

5.5.2 Aufbewahrungsfrist für archivierte Daten

Alle in Abschnitt 5.5.1 genannten archivierten Daten werden während der gesamten Verwendungsdauer des privaten WDR Sub-CA 01 Schlüssels aufbewahrt. Ausnahme bilden die Tickets mit den Sperranträgen für Client-Authentifikationszertifikate. Diese werden mindestens 10 Jahre aufbewahrt.

5.5.3 Schutz der Archive

Das Ersatz-HSM, das als Hot-Standby bereitsteht, wird in einem anderen Rechenzentrum des WDR aufbewahrt bzw. betrieben.

Die Passwort-Briefe mit den Passwörtern für die beiden HSMs, das Pre-Boot-Passwort sowie die Rescue Disk für die Laufwerksverschlüsselung werden in einem Tresor beim WDR sicher verwahrt.

Die Sperranträge von SSL-Server-Administratoren an die WDR Sub-CA 01 werden vom WDR Sub-CA 01 Manager in Papierform sicher verwahrt. Die Tickets mit den Sperranträgen für Client-Authentifikationszertifikate verbleiben im Ticketsystem und werden dort gesichert. Nur berechtigte Administratoren haben schreibenden bzw. löschenden Zugriff auf das Ticketsystem.

Das aktuelle Backup der WDR Sub-CA 01 Zertifikatsdatenbank ist in der täglich erstellten Sicherung von Laufwerk C enthalten und wird „vmware data protection“ gesichert. Nur berechtigte Administratoren haben schreibenden bzw. löschenden Zugriff auf das „vmware data protection“.

Die Log-Dateien der WDR Sub-CA 01 im Ereignisprotokoll sind in der täglich erstellten Sicherung von Laufwerk C enthalten und werden im „vmware data protection“ gesichert. Nur berechtigte Administratoren haben schreibenden bzw. löschenden Zugriff auf das <Backup-System>.

5.5.4 Datensicherung des Archivs

Für den privaten Schlüssel der WDR Sub-CA 01 gibt es keine weiteren Sicherungskopien. Für die im Tresor aufbewahrten Daten erfolgt keine zusätzliche Datensicherung.

5.5.5 Anforderungen an Zeitstempel

Es bestehen keine Anforderungen an Zeitstempel.

5.5.6 Archivierungssystem

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

5.5.7 Prozeduren für Abruf und Überprüfung archivierter Daten

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

5.6 Schlüsselwechsel der Zertifizierungsstelle

Der private Schlüssel der WDR Sub-CA 01 wird nur so lange zum Ausstellen von Endanwender-Zertifikaten eingesetzt, wie die Gültigkeit der untergeordneten Zertifikate noch innerhalb des Gültigkeitsrahmens des WDR Sub-CA 01-Zertifikats liegen (siehe auch Kapitel 6.3.2).

Beim Schlüsselwechsel der WDR Sub-CA 01 wird neues Schlüsselmaterial generiert, das alte Schlüsselmaterial wird nicht beibehalten.

5.7 Kompromittierung und Wiederherstellung

5.7.1 Vorgehen bei Sicherheitsvorfällen und Kompromittierung

Falls im Laufe der Gültigkeitsdauer des WDR Sub-CA 01 Zertifikats die verwendeten Krypto-verfahren bzw. Schlüssellängen (siehe Kapitel 6.1 und 7.1) nicht mehr als hinreichend sicher zu betrachten sind, müssen das Zertifikat der WDR Sub-CA 01 und alle von ihr erstellten Endanwenderzertifikate gesperrt und die WDR Sub-CA 01 durch eine neue WDR Sub-CA 01 ersetzt werden. Zusätzlich wird die CA-Steuerungsgruppe informiert. Die Außerbetriebnahme der bestehenden WDR Sub-CA 01 wird in Abschnitt 5.8 beschrieben. Beim Aufbau einer neuen WDR Sub-CA 01 ist das gesamte Schlüsselmaterial der CA neu zu erzeugen und ein neues Zertifikat bei der WDR RfA-CA zu beantragen. Anschließend müssen alle Endanwenderzertifikate von der WDR Sub-CA 01 neu ausgestellt werden.

5.7.2 Betriebsmittel, Software und/oder Daten sind korrumpiert

Bei versehentlicher Löschung des WDR Sub-CA 01 Schlüssel in dem einen HSM wird der Schlüssel in dem Ersatz-HSM verwendet.

Im Fall korrumpierter Software oder Daten wird die virtuelle Maschine der WDR Sub-CA 01 gelöscht und eine neue virtuelle Maschine für die WDR Sub-CA 01 aufgesetzt, die WDR Sub-CA 01 neu installiert und konfiguriert. In diese neue WDR Sub-CA 01 wird das letzte Backup der WDR Sub-CA 01 Datenbank und Log-Dateien aus dem Backup-System des WDR eingespielt.

Auch für Endanwender gilt: Im Verdachtsfall von kompromittierter PKI-Software oder Daten muss die Software neu installiert werden.

5.7.3 Kompromittierung des privaten Schlüssels

Der private Schlüssel der WDR Sub-CA 01 kann im Normalfall nicht aus dem HSM ausgelesen und somit nicht unbemerkt kopiert werden. Wird bei dem verwendeten HSM

jedoch eine Schwachstelle entdeckt, könnte ggf. dieser Schutz des privaten Schlüssels hinfällig sein. Bei hinreichendem Verdacht auf eine Kompromittierung des privaten Schlüssels der WDR Sub-CA 01 wird von dem WDR Sub-CA 01 Admin eine anlass-bezogene Auswertung des Vorfalls unter Einbindung des IT-Sicherheitsbeauftragten des WDR vorgenommen.

Bei einer Kompromittierung muss das Zertifikat der WDR Sub-CA 01 und alle von ihr erstellten Endanwenderzertifikate gesperrt und die WDR Sub-CA 01 durch eine neue CA ersetzt werden. Die Außerbetriebnahme der bestehenden WDR Sub-CA 01 wird in Abschnitt 5.8 beschrieben.
Beim Aufbau einer neuen WDR Sub-CA 01 ist das gesamte Schlüsselmaterial der CA neu zu generieren und ein neues Zertifikat bei der WDR RfA-CA zu beantragen. Anschließend müssen alle Endanwenderzertifikate von der WDR Sub-CA 01 neu ausgestellt werden.

Auch für Endanwender gilt: Im Verdachtsfall eines kompromittierten privaten Schlüssels muss das Server- bzw. Client-Authentifikationszertifikat des Endanwenders gesperrt, neues Schlüsselmaterial erzeugt und ein neues Zertifikat bei der WDR Sub-CA 01 beantragt werden.

5.7.4 Wiederaufnahme des Betriebs nach einem Notfall

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

5.8 Einstellung des Betriebs

Wenn die WDR Sub-CA 01 ihren Betrieb einstellt, stellt sie einen Sperrantrag für ihr Zertifikat bei der WDR RfA-CA. Mit der Sperrung des WDR Sub-CA 01 Zertifikats werden automatisch auch alle untergeordneten Zertifikate ungültig. Trotzdem sperrt die WDR Sub-CA 01 alle von ihr ausgestellten Zertifikate, die noch gültig sind, stellt anschließend eine letzte Sperrliste aus und veröffentlicht diese. Diese letzte Sperrliste ist bis zum Ende der Laufzeit des WDR Sub-CA 01 Zertifikats gültig. Abschließend werden der private Schlüssel der WDR Sub-CA 01 auf den beiden HSMs sicher gelöscht (siehe Abschnitt 6.2.10).

6 Technische Sicherheitsmaßnahmen

6.1 Schlüsselerzeugung und Installation

6.1.1 Schlüsselerzeugung

Das Schüsselpaar der WDR Sub-CA 01 wurde während der Installation der AD CS in einem HSM erzeugt und anschließend in ein zweites HSM transferiert, das als Hot-Standby bereitsteht. So ist es vor unberechtigtem Zugriff, Löschung und Manipulation geschützt.

Schlüssel von Endanwendern müssen dezentral vom Endanwender selbst oder von einer autorisierten Person/System erzeugt werden wie bspw. einem Server-Administrator oder einem MDM.

6.1.2 Übermittlung privater Schlüssels an Zertifikatsnehmer

Da die Schlüssel der WDR Sub-CA 01 dezentral von der WDR Sub-CA 01 selbst erzeugt wurden, war keine Übermittlung des privaten Schlüssels von der WDR RfA-CA an die WDR Sub-CA 01 notwendig.

Da auch die Schlüssel von Endanwendern nicht zentral von der WDR Sub-CA 01 erzeugt werden, ist auch keine Übermittlung des privaten Schlüssels von der WDR Sub-CA 01 notwendig.

6.1.3 Übermittlung öffentlicher Schlüssels an Zertifikatsaussteller

Der öffentliche Schlüssel der WDR Sub-CA 01 wurde von dem WDR Sub-CA 01 Admin auf einem Transfer-Datenträger persönlich den Administratoren der WDR RfA-CA übergeben. Da der WDR Sub-CA 01 Admin den Administratoren der WDR RfA-CA persönlich bekannt ist, wurde keine Ausweisprüfung durchgeführt.

Zu zertifizierende öffentliche Schlüssel von Endanwendern werden in Form eines signierten Zertifikatsantrags (Certificate Signing Request, CSR) auf vertrauenswürdigem Weg an die WDR Sub-CA 01 übermittelt. Dabei werden zur Übermittlung des öffentlichen Schlüssels eine der von den AD CS angebotenen Schnittstellen verwendet (Auto-Enrollment, Web-Enrollment). Der Antragsteller ist im AD des WDR enthalten und authentifiziert sich vorab bei der Windows-Anmeldung mit seinem AD-Benutzernamen und –Passwort.

6.1.4 Verteilung des öffentlichen CA-Schlüssels an Zertifikatsprüfer

Die beiden CA-Zertifikate mit den öffentlichen Schlüsseln der WDR RfA-CA und der WDR Sub-CA 01 werden im Active Directory, im Daten-CN und im Internet bereitgestellt (siehe Kapitel 2.1). Die URLs, von denen das Zertifikat der WDR RfA-CA abgerufen werden kann, stehen in einer Zertifikatserweiterung im Zertifikat der WDR Sub-CA 01. Die URLs, von denen das Zertifikat der WDR Sub-CA 01 abgerufen werden kann, werden in einer Zertifikatserweiterung in allen ausgestellten Endanwenderzertifikaten vermerkt (siehe Kapitel 7.1.2).

6.1.5 Schlüssellängen

Die WDR Sub-CA 01 nutzt das RSA Kryptoverfahren mit einer Schlüssellänge von 2048 Bit.

Auch die Schlüssel der Endanwender müssen mindestens 2048 Bit lang sein.

6.1.6 Erzeugung der Public Key Parameter und Qualitätssicherung

Die Schlüssel der WDR Sub-CA 01 wurden in einem HSM „Utimaco CryptoServer CSe10LAN“ erzeugt. Dieses HSM ist FIPS 140-2 Level 3 zertifiziert[9].

Bei der Schlüsselerzeugung für Endanwender bestehen keine Anforderung nach FIPS, CC oder einer ähnlichen Zertifizierung.

6.1.7 Schlüsselverwendungszwecke

Das CA-Zertifikat der WDR Sub-CA 01 enthält eine Schlüsselverwendungserweiterung (englisch: KeyUsage Extension) mit den Einträgen Zertifikatssignatur und Sperrlistensignatur (englisch: keyCertSign, cRLSign), d. h. dieses Zertifikat kann zur Unterzeichnung von Zertifikaten und Sperrlisten verwendet werden.

Alle von der WDR Sub-CA 01 ausgestellten Zertifikate für Endanwender sowie die zugehörigen privaten Schlüssel dürfen nur zu den in den Zertifikaten spezifizierten Verwendungszwecken eingesetzt werden (KeyUsage Erweiterung, siehe Kapitel 7.1.2).

Zertifikatsprüfer müssen diese Schlüsselverwendungszwecke prüfen, bevor sie das Zertifikat verwenden dürfen.

9 https://hsm.utimaco.com/de/cryptoserver/securityserver-cse/

6.2 Schutz privater Schlüssel und Einsatz kryptographischer Module

6.2.1 Standard kryptographischer Module

Der private Schlüssel der WDR Sub-CA 01 liegt in einem HSM, dessen Sicherheit und Compliance durch folgende Zertifikate bestätigt wird[9]:

- FIPS 140-2 Level 3, Physikalische Sicherheit Level 4**
- PCI HSM Zertifizierung (durch Drittanbieter)
- DK Zulassung der Deutschen Kreditwirtschaft
- CE, FCC Class B
- UL, IEC/EN 60950-1
- CB Zertifikat
- RoHS II, WEEE

Für die privaten Schlüssel der Endanwender zur WLAN- bzw. SSL-Authentifizierung müssen keine zertifizierten kryptographische Module verwendet werden.

6.2.2 Aufteilung privater Schlüssel auf mehrere Personen

Der private Schlüssel der WDR Sub-CA 01 ist nicht auf mehrere Personen aufgeteilt.

Gleiches gilt für den privaten Schlüssel der Endanwender: Dieser muss nicht auf mehrere Personen aufgeteilt sein.

6.2.3 Hinterlegung privater Schlüssel

Der private Schlüssel der WDR Sub-CA 01 ist nicht hinterlegt (kein Key Escrow).

Die privaten Authentifikationsschlüssel für Server und Clients dürfen auch nicht vom Endanwender bei Anbietern von Key-Escrow-Diensten hinterlegt werden.

6.2.4 Backup privater Schlüssel

Von dem im HSM gespeicherten privaten Schlüssel der WDR Sub-CA 01 wurde eine Sicherungskopie in ein zweites HSM transferiert, das als Hot-Standby bereitsteht.

Die WDR Sub-CA 01 sichert keine privaten Schlüssel der Endanwender.

Die privaten Authentifikationsschlüssel für Server und Clients müssen auch nicht vom Endanwender gesichert werden.

6.2.5 Archivierung privater Schlüssel

Das Ersatz-HSM mit der Sicherungskopie des privaten Schlüssels der WDR Sub-CA 01 befindet sich in einem zweiten Rechenzentrum des WDR.

Der versiegelte Passwortbrief mit dem Partitions-Passwort des Ersatz-HSMs wird in einem Tresor beim WDR aufbewahrt.

Schlüssel von Endanwendern müssen nicht archiviert werden.

6.2.6 Transfer privater Schlüssel in oder aus einem kryptographischen Modul

Der private Schlüssel der WDR Sub-CA 01 wurde in ein zweites HSM transferiert, das als Hot-Standby bereitsteht (siehe Abschnitt 6.2.4).

6.2.7 Speicherung privater Schlüssel in einem kryptographischen Modul

Der private Schlüssel der WDR Sub-CA 01 liegt in dem HSM „Utimaco CryptoServer CSe10LAN“.

Die privaten Schlüssel von Endanwendern können entweder auf Smartcard, in einem TPM oder in Software gespeichert werden.

6.2.8 Aktivierung privater Schlüssel

Die Aktivierung des privaten Schlüssels der WDR Sub-CA 01 im HSM ist nur durch Eingabe des Partitions-Passworts möglich.

Der Zugriff auf den privaten Schlüssel von Systemen (Server oder Maschinen) muss nicht zwingend durch ein Passwort gesichert sein. Dafür muss aber der Zugriff auf die Systeme hinreichend gesichert werden.

Die privaten Benutzerschlüssel von Endanwendern müssen hingegen durch ein geeignetes Passwort vor unautorisiertem Zugriff geschützt werden.

6.2.9 Deaktivierung privater Schlüssel

Der private Schlüssel der WDR Sub-CA 01 bleibt so lange aktiv, wie der Server der WDR Sub-CA 01 in Betrieb ist und Endanwenderzertifikate oder Sperrlisten erstellt. Bei Bedarf kann der private Schlüssel der WDR Sub-CA 01 deaktiviert werden.

Auch private Schlüssel der Endanwender können solange aktiv bleiben wie der Zugriff auf den privaten Schlüssel erforderlich ist. Bei Bedarf muss der private Schlüssel deaktiviert werden können.

6.2.10 Vernichtung privater Schlüssel

Sollte es nötig werden, den privaten Schlüssel der WDR Sub-CA 01 zu löschen, so werden die Schlüssel durch die Löschroutine des HSMs sicher gelöscht.

Der private Schlüssel eines Endanwenderzertifikats muss sicher gelöscht werden, wenn er nicht mehr benötigt wird.

6.2.11 Güte kryptographischer Module

Das verwendete HSM ist nach FIPS 140-2 Level 3 zertifiziert (siehe Kapitel 6.2.1).

Die Endanwender müssen keine zertifizierten kryptographischen Module zur Speicherung ihrer privaten Schlüssel verwenden.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel werden nicht archiviert.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Das von der WDR RfA-CA ausgestellte WDR Sub-CA 01 Zertifikat ist ab dem Ausstellungszeitpunkt 10 Jahre, d. h. bis 2025 gültig. Der zugehörige private Schlüssel der WDR Sub-CA 01 wird aber keine 10 Jahre zur Ausstellung von Endanwenderzertifikaten genutzt, da Endanwenderzertifikate nicht länger gültig sein dürfen als das Zertifikat der ausstellenden CA. Die von der WDR Sub-CA 01 auszustellenden Zertifikate sind maximal zwei Jahre gültig. Somit ergibt sich eine Verwendungsdauer des privaten Schlüssels der WDR Sub-CA 01 von maximal acht Jahren. In den letzten zwei Jahren seiner Laufzeit wird er nicht mehr zur Ausstellung weiterer Endanwenderzertifikate genutzt, sondern nur noch zur Ausstellung von Sperrlisten.

OCSP-Responder-Zertifikate sind nur zwei Wochen gültig, da diese nicht auf Sperrung geprüft werden[10].

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation der Aktivierungsdaten

Die Aktivierung des privaten Schlüssels der WDR Sub-CA 01 erfordert die Eingabe des Partitionspassworts für das HSM. Dieses Passwort wurde bei der Initialisierung des HSMs vergeben. Es ist 12 Zeichen lang.

Zur Aktivierung eines Endanwenderschlüssels zur Server- oder Maschinenauthentifikation ist kein Passwort oder PIN erforderlich.
Für private Benutzerschlüssel von Endanwendern muss bei der Erzeugung und Installation des Schlüsselmaterials ein geeignetes Passwort bzw. PIN vergeben werden.

6.4.2 Schutz der Aktivierungsdaten

Das Partitionspasswort ist nur dem WDR Sub-CA 01 CA Administrator und dem WDR Sub-CA 01 CA Manager bekannt. Außerdem ist es in einem Tresor beim WDR hinterlegt.

Das Passwort bzw. die PIN zum Schutz vor unautorisiertem Zugriff auf den privaten Benutzerschlüssel von Endanwendern darf nur dem Endanwender selbst bekannt sein. Er darf diese Aktivierungsdaten nicht weitergeben.

6.4.3 Weitere Aspekte

Keine weiteren Festlegungen.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Die WDR Sub-CA 01 wird auf einem Windows Server 2012 R2 im Enterprise-CA Modus betrieben. Dieser Server läuft als virtuelle Maschine in der zentralen VMware Infrastruktur beim WDR. Als Betriebssystem ist in der VM – entsprechend den hierfür gültigen Vorgaben des WDR – Windows Server 2012 R2 Standard Edition installiert. Dieser Server ist im AD integriert.

Zugriff auf die VM mit der WDR Sub-CA 01 erfolgt über einen Arbeitsplatzrechner, auf dem alle aktuellen Windows-Patches, ein aktueller Virenscanner und ein VMware vSphere Client oder ein Server Manager (Remote Server Administration Tools for Windows 8.1) installiert sind. Alternativ kann der Zugriff auf die WDR Sub-CA 01 VM auch über RDP erfolgen.

Die WDR Sub-CA 01 wird durch geeignete Benutzerauthentisierung und Zugriffskontrolle vor unberechtigten Zugriffen geschützt. Sowohl der Lokale System Administrator als auch der WDR Sub-CA 01 Admin und der WDR Sub-CA 01 Manager haben ein Passwort bestehend aus 12 Zeichen. Weitere Benutzer haben keinen Zugriff auf die VM.

Für die zentralen Komponenten der WDR Sub-CA 01 gelten dieselben IT-Sicherheits-anforderungen wie für die anderen Serversysteme beim WDR.

---

10 Eine Sperrprüfung des OCSP-Responder-Zertifikats per OCSP würde zur Endlosrekursion führen. Eine Sperrprüfung per CRL würde den Einsparungseffekt durch OCSP ad absurdum führen. OCSP-Responder Zertifikate sind durch eine OCSPNoCheck-Erweiterung gekennzeichnet.

6.5.2 Beurteilung von Computersicherheit

Für den Server gibt es keine Gütesiegel in Form von Zertifikaten wie bspw. eine CC-Evaluierung und Bestätigung.

Auch für die Systeme und Maschinen der Endanwender besteht keine Anforderung nach einer Beurteilung der Computersicherheit.

6.6 Technische Maßnahmen im Lebenszyklus

6.6.1 Maßnahmen der Systementwicklung

Keine weiteren Festlegungen. Es findet keine Entwicklung statt.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Die Software der WDR Sub-CA 01 wurde in das Patch-Management des WDR aufgenommen. Schwachstellen bei den eingesetzten Systemen werden nach Bekanntwerden der Schwachstelle und Vorliegen eines Patches umgehend behoben.

Für das Betriebssystem auf dem Host und in der VM werden regelmäßig alle aktuellen Updates und Patches eingespielt.

Die gleiche Anforderung gilt auch für Endanwender: Für ihr Betriebssystem müssen auch regelmäßig alle aktuellen Updates und Patches eingespielt werden.

6.6.3 Lebenszyklus der Sicherheitsmaßnahmen

Für den Server der WDR Sub-CA 01 gilt der gleichen Lebenszyklus der Sicherheitsmaßnahmen wie für alle anderen Serversysteme beim WDR auch.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Der Server der WDR Sub-CA 01 ist geeignet vor Zugriffen von außen geschützt. Sämtliche nicht benötigte Netzdienste wurden deaktiviert.

6.8 Zeitstempel

Innerhalb der WDR PKI wird kein Zeitstempeldienst betrieben.

7 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen

7.1 Zertifikatsprofil

7.1.1 Versionsnummer

Die WDR Sub-CA 01 stellt ausschließlich X.509 Zertifikate in Version 3 aus, d.h. die Versionsnummer im Zertifikat ist auf den Wert 2 gesetzt.

7.1.2 Zertifikatserweiterungen

In den von der WDR Sub-CA 01 ausgestellten Authentisierungszertifikaten für Systeme (Server und Maschinen) sind folgende Zertifikatserweiterungen enthalten:

- KeyUsage (Schlüsselverwendung)
- CRLDistributionPoints (Sperrlisten-Verteilungspunkte)
- AuthorityInfoAccess (Adresse des OCSP Responders)
- AuthorityKeyIdentifier (Stellenschlüsselkennung)
- SubjectKeyIdentifier (Schlüsselkennung des Antragstellers)

- SubjectAltName (Alternativer Antragstellername)
- ExtendedKeyUsage (Erweiterte Schlüsselverwendung)

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

Optional können außerdem weitere nicht kritische Zertifikatserweiterungen in den Zertifikaten für Endanwender und Systeme ergänzt werden wie bspw. CertificatePolices (Zertifikatrichtlinien).

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

- Certificate Policy: 1.3.6.1.4.1.42638.2.1

Die Certificate Policy Erweiterung ist als nicht-kritisch markiert.

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

- SubjectAltName: E-Mail Adresse und UPN des Benutzers

Die SubjectAltName Erweiterung ist als nicht-kritisch markiert.

OCSP-Responder-Zertifikate:
Für OCSP-Responder-Zertifikate gelten besondere Anforderungen und Einschränkungen bzgl. der Erweiterungen: Es sind mindestens folgende Zertifikatserweiterungen enthalten:

- KeyUsage (Schlüsselverwendung)
- ExtendedKeyUsage (Erweiterte Schlüsselverwendung)
- OCSP No Revocation Checking (1.3.6.1.5.5.7.48.1.5)

Die KeyUsage ist auch hier als kritisch, alle anderen Erweiterungen sind als nicht-kritisch markiert. Als ExtendedKeyUsage ist OCSP Signing (1.3.6.1.5.5.7.3.9) angegeben.

Optional können weitere nicht kritische Zertifikatserweiterungen in den Zertifikaten für OCSP-Responder ergänzt werden. Wegen der „OCSP No Revocation Checking“-Erweiterung werden die CRLDistributionPoints- und die AuthorityInfoAccess-Erweiterung nicht verwendet.

7.1.3 Algorithmus Bezeichner

Es wird der Signaturalgorithmus „sha256WithRSAEncryption“ verwendet.

7.1.4 Namensformen

Siehe Kapitel 3.1.

7.1.5 Namensbeschränkungen

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

7.1.6 Bezeichner für Zertifizierungsrichtlinien

WLAN-Clientzertifikate (Maschinenzertifikaten) enthalten einen RfA-weit einheitlichen Certificate Policy-Identifier (siehe Abschnitt 7.1.2).

7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkungen

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

7.1.8 Syntax und Semantik von Policy Qualifiern

Es werden keine Policy Qualifier – als Bestandteil der CertificatePolicies Erweiterung – verwendet.

7.1.9 Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien

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

7.2 Sperrlistenprofil

7.2.1 Versionsnummer

Die WDR Sub-CA 01 stellt ausschließlich X.509 Sperrlisten in Version 2 aus, d.h. die Versionsnummer im Zertifikat ist auf den Wert 1 gesetzt.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

In den Sperrlisten der WDR Sub-CA 01 sind mindestens folgende Erweiterungen enthalten:

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

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

7.3 OCSP Profil

Die WDR Sub-CA 01 betreibt zusätzlich zur Bereitstellung von Sperrlisten auch einen OCSP-Responder.

Da die OCSP-Responder-Zertifikate von den Endanwendern nicht geprüft werden sollen[11], dürfen OCSP-Responder-Zertifikate nur mit einer kurzen Gültigkeit ausgestellt werden, d. h. sie müssen häufig erneuert werden. Die OCSP-Responder-Zertifikate sind zwei Wochen gültig.

7.3.1 Versionsnummer

Es werden OCSP Basic Responses in Version 1 verwendet, d. h. die Versionsnummer der Response ist auf den Wert 0 gesetzt. Der OCSP Dienst nutzt das Lightweight OCSP Profil nach RFC 5019.

7.3.2 OCSP Erweiterungen

In einer „OCSP Single Response“ ist mindestens folgende Erweiterung enthalten:

- NextCRLPublish (Nächste Sperrlistenveröffentlichung)

Diese OCSP-Single Response-Erweiterung ist als nicht kritisch markiert. Optional können weitere nicht kritische Erweiterungen ergänzt werden.

---

11 Dies wird durch die „OCSP No Revocation Checking“-Erweiterung im OCSP-Responder-Zertifikat reguliert, siehe Kapitel 7.3.2.

NextCRLPublish gibt den Zeitpunkt der nächsten regulär zu erwartenden Veröffentlichung von Sperrinformation an. Er ist identisch mit dem Wert der gleichlautenden Erweiterung der zu Grunde liegenden Sperrliste.

Falls im OCSP Request eine Nonce-Erweiterung enthalten war, wird deren Wert in der OCSP Response übernommen, d. h. in einer OCSP Response ist ggf. folgende Erweiterung enthalten:

- Nonce

8 Konformitätsprüfung (Audit)

Eine Evaluierung der WDR Sub-CA 01 nach Common Criteria, ITSEC, FIPS PUB 140.2 oder nach einem ähnlichen Standard ist nicht vorgesehen.

8.1 Häufigkeit und Bedingungen für Überprüfungen

System- und Anwendungsereignisse, die im Zusammenhang mit der WDR Sub-CA 01 stehen, werden anhand der Log-Dateien bei Verdachtsmomenten überprüft. Zusätzlich werden jährlich - analog zu anderen Systemen der WDR IT-Infrastruktur - durch ein internes Audit die aufgezeichneten System- und Anwendungsereignisse sowie die Prozesse der WDR Sub-CA 01 stichprobenhaft überprüft.

8.2 Identität/Qualifikation des Prüfers

Der Prüfer der WDR Sub-CA 01 verfügt über eine geeignete Qualifikation als Auditor.

8.3 Stellung des Prüfers zum Bewertungsgegenstand

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

8.4 Durch Überprüfungen abgedeckte Themen

Folgende Bereiche werden im Rahmen der Konformitätsprüfung mindestens untersucht:

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

8.5 Reaktionen auf Unzulänglichkeiten

Wurden im Rahmen der Prüfung Mängel festgestellt, bewertet der IT-Sicherheitsbeauftragte des WDR die Prüfungsergebnisse mit dem WDR Sub-CA 01 Admin und dem WDR Sub-CA Manager gemeinsam und entscheidet über das weitere Vorgehen. Die festgestellten Mängel werden priorisiert und geeignete Korrekturmaßnahmen prioritätengesteuert eingeleitet und koordiniert.

8.6 Information über Bewertungsergebnisse

Die Ergebnisse des Audits werden dem Betreiber der WDR RfA-CA zur Verfügung gestellt.

9 Andere geschäftliche und rechtliche Angelegenheiten

9.1 Gebühren

Für die Nutzung der WDR Sub-CA 01 werden keine Gebühren erhoben.

9.2 Finanzielle Verantwortung

Finanzielle Aspekte werden in diesem Dokument nicht beschrieben.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Definition von vertraulichen Informationen

Jegliche Informationen über Teilnehmer und Antragsteller, die nicht unter den nächsten Abschnitt fallen, werden als vertrauliche Informationen eingestuft und behandelt.

9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören

Alle Informationen, die in den veröffentlichten Zertifikaten, Sperrlisten und OCSP-Auskünften enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft. Hierzu zählt z. B. der Name und Betreiber der WDR Sub-CA 01.

9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen

Die WDR Sub-CA 01 trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen. Daten dürfen im Rahmen der Diensterbringung nur weitergegeben werden, wenn zuvor eine Vertraulichkeitserklärung unterzeichnet wurde und die mit den Aufgaben betrauten Mitarbeiter auf Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet wurden.

9.4 Schutz personenbezogener Daten

9.4.1 Datenschutzkonzept

Zur Leistungserbringung werden von der WDR Sub-CA 01 personenbezogene Daten elektronisch gespeichert und verarbeitet. Dies geschieht in Übereinstimmung mit den entsprechenden Gesetzen.

9.4.2 Als persönlich behandelte Daten

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.1 analog.

9.4.3 Daten, die nicht als persönlich behandelt werden

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.2 analog.

9.4.4 Zuständigkeiten für den Datenschutz

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.3 analog.

9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten

Der Zertifikatsnehmer stimmt der Nutzung von personenbezogenen Daten durch die WDR Sub-CA 01 zu, soweit dies zur Leistungserbringung erforderlich ist. Darüber hinaus können alle Informationen veröffentlicht werden, die als nicht vertraulich behandelt werden (siehe Abschnitt 9.4.3) und deren Veröffentlichung nicht widersprochen wurde.

9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften

Die WDR Sub-CA 01 unterliegt deutschem Recht und gibt vertrauliche und personenbezogene Informationen an staatliche Organe beim Vorliegen entsprechender Entscheidungen in Übereinstimmung mit den geltenden Gesetzen frei.

9.4.7 Andere Bedingungen für Auskünfte

Es sind keine weiteren Umstände für eine Veröffentlichung vorgesehen.

9.5 Urheberrechte

Keine weiteren Festlegungen.

9.6 Verpflichtungen

9.6.1 Zusicherungen und Garantien der CA

Die WDR Sub-CA 01 verpflichtet sich, die Anforderungen dieses kombinierten CP/CPS-Dokuments geeignet umzusetzen und ihre Aufgaben nach bestem Wissen und Gewissen durchzuführen.

9.6.2 Zusicherungen und Garantien der RA

Keine weiteren Festlegungen. Es gibt keine Registrierungsstelle (siehe Abschnitt 1.3.2).

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

Es bestehen keine Zusicherungen und Garantien anderer Zertifikatsinfrastruktur-Teilnehmer.

9.7 Gewährleistung

Keine weiteren Festlegungen.

9.8 Haftungsbeschränkung

Keine weiteren Festlegungen.

9.9 Haftungsfreistellung

Keine weiteren Festlegungen.

9.10 Inkrafttreten und Aufhebung

9.10.1 Gültigkeitsdauer

Dieses kombinierte CP/CPS-Dokument tritt nach Veröffentlichung in Kraft.

9.10.2 Beendigung

Dieses kombinierte CP/CPS-Dokument ist solange gültig, bis es durch eine neue Version ersetzt wird oder der Betrieb der WDR Sub-CA 01 eingestellt wird. Die jeweils gültige Version dieses Dokuments wird im auf der Webseite wdrmspki.wdr.de veröffentlicht.

9.10.3 Auswirkung der Beendigung und Weiterbestehen

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

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

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

9.12 Änderungen der Richtlinie

Die Erweiterung oder Modifikation dieses Dokuments liegt in der Verantwortung des Betreibers der WDR Sub-CA 01 als Inhaber dieses kombinierten CP/CPS-Dokuments.

9.13 Konfliktbeilegung

Keine weiteren Festlegungen.

9.14 Geltendes Recht

Der Betrieb der WDR Sub-CA 01 unterliegt den Gesetzen der Bundesrepublik Deutschland.

9.15 Konformität mit geltendem Recht

Die WDR Sub-CA 01 ist kein Zertifizierungsdienstanbieter im Sinne des deutschen Signaturgesetzes und stellt keine qualifizierten Zertifikate aus. Es werden allenfalls Zertifikate ausgestellt, mit denen fortgeschrittene elektronische Signaturen gemäß dem deutschen Signaturgesetz erzeugt werden können.

9.16 Weitere Regelungen

9.16.1 Vollständigkeitserklärung

Die Ausgabe einer neuen Version dieses kombinierten CP/CPS-Dokuments ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2 Abgrenzungen

Keine weiteren Festlegungen.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses kombinierten CP/CPS-Dokuments unwirksam sein, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Anstelle der unwirksamen Bestimmungen gilt diejenige wirksame Bestimmung als vereinbart, welche dem Sinn und Zweck der unwirksamen Bestimmung weitgehend entspricht.

9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

Rechtliche Auseinandersetzungen, die aus dem Betrieb der WDR Sub-CA 01 herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland. Erfüllungsort und ausschließlicher Gerichtsstand ist der Sitz des Betreibers.

9.16.5 Höhere Gewalt

Keine weiteren Festlegungen.

9.17 Andere Regelungen

Keine weiteren Festlegungen.