Trustcenter der
Deutschen Rentenversicherung

Certificate Policy
und
Certification Practice Statement
der
Wurzelzertifizierungsstelle
der Deutschen Rentenversicherung

Version 5.0

Stand 28.01.11

Inhalt

1 Einleitung 5
1.1 Überblick 5
1.2 Zielsetzung dieses Dokumentes 5
1.3 Dokumentidentifikation 6
1.4 Teilnehmer und Instanzen des Trustcenters 6
1.4.1 Zertifizierungsstelle und -instanzen 6
1.4.2 Registrierungsinstanzen 6
1.4.3 Zertifikatswerber 6
1.4.4 Zertifikatsinhaber 7
1.5 Anwendung von Zertifikaten 7
1.5.1 Vorgesehene Anwendung von Zertifikaten 7
1.5.2 Nicht vorgesehene Zertifikatsverwendung 7
1.6 Verwaltung dieses Dokumentes 7
1.6.1 Organisation für die Verwaltung dieses Dokuments 7
1.6.2 Kontaktperson 7
1.6.3 Verantwortlicher für die Anerkennung anderer CPS 7
1.6.4 Genehmigungsverfahren für die Anerkennung anderer CPS 7
1.7 Abkürzungen 7

2 Prozesse zur Erstellung von Zertifikaten 9
2.1 CA-Zertifikate für Wurzel- und Mitarbeiter-CAs 9
2.1.1 Registrierung 9
2.1.2 Key-Ceremony 9
2.1.3 Sperrung 10
2.1.4 Schlüsselerneuerung 10
2.1.5 Archivierung 10
2.2 OCSP-Signer-Zertifikate für Wurzel- und Mitarbeiter-CAs 11
2.2.1 Registrierung 11
2.2.2 Key-Ceremony 11
2.2.3 Sperrung 11
2.2.4 Schlüsselerneuerung 12
2.2.5 Archivierung 12
2.3 TSP-Signer-Zertifikate 12
2.3.1 Registrierung 12
2.3.2 Key-Ceremony 12
2.3.3 Sperrung 13
2.3.4 Schlüsselerneuerung 13
2.3.5 Archivierung 13
2.4 CA-Zertifikate für Server-CAs 13
2.4.1 Registrierung 13
2.4.2 Key-Ceremony 14
2.4.3 Sperrung 14
2.4.4 Schlüsselerneuerung 15
2.4.5 Archivierung 15
2.5 OCSP-Signer-Zertifikate der Server-CAs 15
2.5.1 Registrierung 15
2.5.2 Key-Ceremony 16
2.5.3 Sperrung 16
2.5.4 Schlüsselerneuerung 16
2.5.5 Archivierung 16

3 Ausführende Rollen 17

4 Bekanntmachung und Verzeichnisdienst 19

4.1 Verzeichnisdienst 19
4.1.1 LDAP-Verzeichnisdienst 19
4.1.2 OCSP-Responder 19
4.2 Veröffentlichung von Informationen der PKI-Instanzen 20
4.3 Häufigkeit und Zyklen für Veröffentlichungen 20

5 Namenskonzept 21
5.1 Eindeutigkeit von Namen 21
5.2 Anonymität und Pseudonyme für Zertifikatseigentümer 21

6 Prüfung des Zertifikatsstatus durch Dritte 22

7 Sicherheitsmaßnahmen 23
7.1 Sicherheitsziele 23
7.2 Gesetzliche Anforderungen 23
7.3 Personelle Sicherheitsmaßnahmen 23
7.4 Prozessbezogene Sicherheitsmaßnahmen 24
7.4.1 Rollentrennung 24
7.4.2 Rollentrennung im Bereich der administrativen Rollen 24
7.4.3 Vertretungsregelung 24
7.4.4 Rufbereitschaft 24
7.5 Technische Sicherheitsmaßnahmen 24
7.6 Dokumentation 25
7.7 Melden sicherheitsrelevanter Vorfälle 25

8 Weitere geschäftliche und rechtliche Regelungen 26
8.1 Abschluss einer Verwaltungsvereinbarung 26
8.2 Vertraulichkeit personenbezogener Informationen 26
8.3 Haftung des Zertifizierungsdiensteanbieters 26
8.4 Pflichten der Zertifikatsinhaber 26
8.5 Gültigkeit dieses Dokumentes 26
8.5.1 Gültigkeitszeitraum 26
8.5.2 Vorzeitiger Ablauf der Gültigkeit 26
8.6 Änderungen / Ergänzungen dieses Dokumentes 26
8.6.1 Verfahren für die Änderung / Ergänzung dieses Dokumentes 26
8.6.2 Benachrichtigungsverfahren und Veröffentlichungsperioden 26
8.6.3 Änderungsbedingungen 27
8.6.4 Schriftlichkeitsgebot 27

9 Zertifikatsprofile 28
9.1 Zertifikate der Wurzel-CAs 29
9.1.1 Zertifikat der QC Root CA 29
9.1.2 Zertifikat der NQ Root CA 30
9.2 CRL-Signer-Zertifikate 31
9.2.1 CRL-Signer-Zertifikat der QC Root CA 31
9.3 OCSP-Signer-Zertifikate und TSP-Signer-Zertifikate der Wurzel-CAs 33
9.3.1 OCSP-Signer-Zertifikat der QC Root CA 33
9.3.2 OCSP-Signer-Zertifikat der NQ Root CA 36
9.3.3 TSP-Signer-Zertifikat der QC Root CA 38
9.4 Zertifikate der Mitarbeiter-CAs 41
9.4.1 Zertifikat der QC <RVTNR> Mitarbeiter CA 41
9.4.2 Zertifikat der NQ <RVTNR> Mitarbeiter CA 44
9.5 Zertifikate der Server-CAs 46
9.5.1 Zertifikat der NQ DRV CA 46
9.5.2 Zertifikat der NQ DRV WAN01 CA 48

10 CRLs 50
10.1 CRL der QC Root CA 50
10.2 Delta-CRL der QC Root CA 52

10.3 CRL der NQ Root CA 54
10.4 Delta-CRL der NQ Root CA 56

11 Verzeichnisse 58
11.1 Tabellenverzeichnis 58

1 Einleitung

1.1 Überblick

Die Träger der Deutschen Rentenversicherung betreiben nach § 138 SGB VI ein gemeinschaftliches Trustcenter zur Bereitstellung von Zertifizierungsdiensten nach dem deutschen Signaturgesetz. Jeder RV-Träger, der sich dem Trustcenter der Deutschen Rentenversicherung anschließt, tritt als ein bei der Bundesnetzagentur nach dem SigG angezeigter Zertifizierungsdiensteanbieter auf. Mit dieser Anzeige unterliegt jeder Zertifizierungsdiensteanbieter der Deutschen Rentenversicherung auch bestimmten Haftungsregelungen. Zudem kann die Bundesnetzagentur dort jederzeit die Einhaltung der Regelungen des Signaturgesetzes prüfen.

Das Trustcenter der Deutschen Rentenversicherung ist so aufgebaut, dass es gegebenenfalls auch für Träger aus weiteren Bereichen der Sozialversicherung und der öffentlichen Verwaltung zentrale Trustcenter-Funktionen übernehmen kann.

Unter einer zentral vollständig bei der Deutschen Rentenversicherung Bund betriebenen Wurzelzertifizierungsstelle werden für jeden angeschlossenen RV-Träger Zertifizierungsstellen betrieben.

In der Wurzelzertifizierungsstelle wird einerseits eine Wurzel für qualifizierte Zertifikate und andererseits eine Wurzel für fortgeschrittene Zertifikate betrieben. Die Wurzelzertifizierungsstelle für qualifizierte Signaturzertifikate ist bei der Bundesnetzagentur angezeigt.

Die von der Wurzelzertifizierungsstelle ausgestellten Wurzel-Zertifikate bilden den Vertrauensanker der Zertifikatshierarchie des Trustcenters der Deutschen Rentenversicherung.

Jede Zertifizierungsstelle eines RV-Trägers besitzt eigene Signaturerstellungseinheiten und Zertifikate für das Signieren beantragter Benutzerzertifikate und von Zertifikats-Statusauskünften des OCSP-Verzeichnisdienstes. Die Wurzelzertifizierungsstelle verwaltet diese Signaturerstellungseinheiten und erzeugt Zertifikate der Zertifizierungsstellen der RV-Träger. Die Zertifizierungsstellen eines RV-Trägers wiederum stellen Zertifikate und Chipkarten für dessen Mitarbeiter aus und verwalten diese.

Die Wurzelzertifizierungsstelle stellt außerdem auch qualifizierte Zertifikate für den Zeitstempeldienst der Deutschen Rentenversicherung aus und verwaltet dessen Signaturerstellungseinheiten. Dieser Zeitstempeldienst erstellt Zeitstempel im Sinne des § 2 Nr. 14 SigG.

Die Wurzelzertifizierungsstelle stellt weiterhin fortgeschrittene Zertifikate für verschiedene Server-CAs aus.

1.2 Zielsetzung dieses Dokumentes

Dieses Dokument ist Certificate Policy und Certification Practice Statement gleichzeitig.

Der Begriff „Certificate Policy“ steht für die Gesamtheit der Regeln und Vorgaben, welche die Anwendbarkeit eines Zertifikatstyps festlegen. Die Zielsetzung einer Certificate Policy ist im RFC 3647, „Certificate Policy and Certification Practices Framework“, ausführlich dargestellt. Insbesondere sollte eine Certificate Policy darlegen,

- welche technischen und organisatorischen Anforderungen die bei der Ausstellung der Zertifikate eingesetzten Systeme und Prozesse erfüllen,
- welche Vorgaben für die Anwendung der Zertifikate sowie im Umgang mit den zugehörigen Schlüsseln und Signaturerstellungseinheiten (zum Beispiel Chipkarten) gelten,

- welche Bedeutung den Zertifikaten und ihrer Anwendung zukommt, das heißt welche Sicherheit, Beweiskraft, oder rechtliche Relevanz die mit ihnen erzeugten Kryptogramme bzw. Signaturen besitzen.

Nach RFC 3647 legt das „Certification Practice Statement“ (CPS) die Praktiken dar, die ein Trustcenter bei der Ausgabe der Zertifikate anwendet. Dem entsprechend beschreibt dieses Dokument das Vorgehen der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung bei der Beantragung, Generierung, Auslieferung und Verwaltung der Zertifikate für die Zertifizierungsstellen der Deutschen Rentenversicherung. Das CPS dient der Information des Anwenderkreises der Zertifikate und der Dokumentation von Vorgangsweisen. Das Dokument enthält keine Bestimmungen, die Rechte oder Pflichten von Personen begründen, ändern oder aufheben würden.

1.3 Dokumentidentifikation

Genaue Bezeichnung des Dokuments:

„Certificate Policy und Certification Practice Statement der
Wurzelzertifizierungsstelle der Deutschen Rentenversicherung
Version 5.0“

Die ASN.1 Object Identifier (OID) für dieses Dokument sind:

1.3.6.1.4.1.22204.1.8.1.1.1

und

1.3.6.1.4.1.22204.1.8.2.1.1

1.4 Teilnehmer und Instanzen des Trustcenters

1.4.1 Zertifizierungsstelle und -instanzen

Die Deutsche Rentenversicherung Bund betreibt eine Wurzelzertifizierungsstelle für die Ausgabe von Zertifikaten an Zertifizierungsstellen der Rentenversicherung (Mitarbeiter-CAs, Server-CAs) sowie an den Zeitstempeldienst der Deutschen Rentenversicherung. Die Wurzelzertifizierungsstelle der Deutschen Rentenversicherung verwendet für die Erstellung der Zertifikate ein zentrales Zertifizierungssystem mit jeweils einer CA für qualifizierte und einer CA für fortgeschrittene Zertifikate.

Die Schlüssel, mit denen die beiden CAs der Wurzelzertifizierungsstelle (die eine für qualifizierte Zertifikate, die andere für fortgeschrittene Zertifikate) Zertifikate unterzeichnen, sind die grundlegenden „Vertrauensanker“ der Hierarchie. Über diese Schlüssel stellt jede Wurzelzertifizierungsstelle selbstsignierte Zertifikate aus.

1.4.2 Registrierungsinstanzen

Die Registrierung erfolgt durch die Wurzelzertifizierungsstelle der Deutschen Rentenversicherung.

1.4.3 Zertifikatswerber

Erwerber von Zertifikaten sind die RV-Träger. Die Zertifikate werden vom zentral bei der Deutschen Rentenversicherung Bund betriebenen Zertifizierungsdienst ausgestellt und an die technisch dort platzierten CA vergeben. Weiterhin sind jeder Zertifizierungsstelle mehrere Verzeichnisdienstschlüssel (OCSP-Signer) zugeordnet.

Bis zum 23.01.2009 war jeder qualifizierten CA ein Schlüssel zum Signieren von Sperrlisten zugeordnet (CRL-Signer). Das Zertifikat für einen CRL-Signer wurde von der CA ausgestellt, für die die Sperrlisten signiert werden sollten.

Ab dem Jahr 2011 ergeben sich Änderungen bei der Ausstellung von OCSP- und TSP-Signer-Zertifikaten, die in den Abschnitten 2.2 und 2.3 beschrieben sind.

1.4.4 Zertifikatsinhaber

Zertifikatsinhaber für die Zertifikate der Wurzelzertifizierungsstelle sowie der Server-CAs ist der Leiter der Wurzelzertifizierungsstelle.
Zertifikatsinhaber für die Mitarbeiter-CA-Zertifikate ist auf Grund vertraglicher Vereinbarungen mit dem jeweiligen ZDA ebenfalls der Leiter der Wurzelzertifizierungsstelle.

Zertifikatsinhaber für die übrigen Zertifikate sind auf Grund vertraglicher Vereinbarungen mit dem jeweiligen ZDA die Systemverwalter der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung.

1.5 Anwendung von Zertifikaten

1.5.1 Vorgesehene Anwendung von Zertifikaten

Die Zertifikate der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung Bund dienen dem Betrieb von Zertifizierungsstellen der Deutschen Rentenversicherung und dem Betrieb des Zeitstempeldienstes der Deutschen Rentenversicherung.

1.5.2 Nicht vorgesehene Zertifikatsverwendung

Die Verwendung der Zertifikate für andere als die in diesem Dokument genannten Zwecke ist nicht vorgesehen.

1.6 Verwaltung dieses Dokumentes

1.6.1 Organisation für die Verwaltung dieses Dokuments

Für die Verwaltung dieses Dokumentes ist die Deutsche Rentenversicherung Bund zuständig.

1.6.2 Kontaktperson

Folgender Ansprechweg hinsichtlich dieses Dokumentes besteht:

Deutsche Rentenversicherung Bund
Abteilung Organisation und IT-Services
Trustcenter der Deutschen Rentenversicherung
10704 Berlin

1.6.3 Verantwortlicher für die Anerkennung anderer CPS

Die Anerkennung anderer CPS ist nicht vorgesehen.

1.6.4 Genehmigungsverfahren für die Anerkennung anderer CPS

Die Anerkennung anderer CPS ist nicht vorgesehen.

1.7 Abkürzungen

ASN	Abstract Syntax Notation
BDSG	Bundesdatenschutzgesetz
C	Country
CA	Certification Authority
CERTSN	Zertifikatsseriennummer
CM	Certificate Manager (Zertifizierungssystem)
CN	Common Name
CC	Common Criteria
CP	Certificate Policy
CPS	Certification Practice Statement

CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
Delta-CRL	Aktualisierte Daten einer CRL
DN	Distinguished Name
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ID	Identificator
IETF	Internet Engineering Task Force
IT	Informationstechnik
LDAP	Lightwight Directory Access Protocol
MA	Mitarbeiter
NQ	fortgeschritten
O	Organization
OCF	Open Card Framework
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PIN	Personal Identification Number
PKCS	Public-Key-Cryptosystem
QC	qualifiziert
RFC	Request for Comments - Internet Standards der IETF
RSA	Kryptoalgorithmus von Rivest, Shamir und Adleman
RV	Rentenversicherung
SCEP	Simple Certificate Enrollment Protocol
SGB	Sozialgesetzbuch
SHA	Secure-Hash-Standard (FIPS 180-1)
SigG	Deutsches Signaturgesetz
SigV	Deutsche Signaturverordnung
URL	Unified Ressource Locator
X.509	ITU-Standard für Zertifikate und Sperrlisten
ZDA	Zertifizierungsdiensteanbieter

2 Prozesse zur Erstellung von Zertifikaten

2.1 CA-Zertifikate für Wurzel- und Mitarbeiter-CAs

2.1.1 Registrierung

Zertifikatsinhaber für die Zertifikate der Wurzelzertifizierungsstelle ist der Leiter der Wurzelzertifizierungsstelle.

Der Leiter der Wurzelzertifizierungsstelle ist außerdem Zertifikatsinhaber für alle Zertifikate der Mitarbeiter-CAs. Dadurch wird ermöglicht, dass eine Ausstellung von CA-Zertifikaten oder ein Wiederaufsetzen der CA möglich sind, ohne dass in jedem Fall Personal der RV-Träger zum Standort des Trustcenters anreisen muss.

Der Sicherheitsbeauftragte der Deutschen Rentenversicherung Bund identifiziert den Leiter der Wurzelzertifizierungsstelle und erhebt folgende personenbezogene Daten aus dem Personalausweis bzw. Reisepass und trägt sie in das Protokoll Betriebsaufnahme ein:

- Name
- Vorname
- Geburtsdatum
- Geburtsort
- Staatsangehörigkeit

Der Sicherheitsbeauftragte der Deutschen Rentenversicherung Bund erhebt die Personenkennziffer aus dem Dienstausweis und trägt sie in das Protokoll Betriebsaufnahme bzw. Schlüsselwechsel ein.

Der Leiter der Wurzelzertifizierungsstelle unterzeichnet eine vertragliche Vereinbarung mit dem jeweiligen RV-Träger, dass er auf die Sperrung der Systemzertifikate verzichtet und dem öffentlichen Abruf der Systemzertifikate zustimmt. Er wird in der gleichen Vereinbarung von der Haftung durch Missbrauch der Systemschlüssel freigestellt.

2.1.2 Key-Ceremony

Alle CA-Schlüssel der qualifizierten CAs werden auf sicheren Signaturerstellungseinheiten (Systemchipkarten) betrieben. Alle CA-Signer-Schlüssel der fortgeschrittenen CA werden auf HSMs betrieben, deren Sicherheit sich an den Vorgaben des Signaturgesetzes orientiert. Bis zum 23.01.2009 wurden CRL-Signer-Schlüssel für qualifizierte CAs verwendet und ebenfalls auf solchen HSMs betrieben.

Die Wurzelzertifizierungsstelle der Deutschen Rentenversicherung personalisiert bei der Betriebsaufnahme, jährlich bei der Schlüsselerneuerung und bei notwendigen Ersatzleistungen Systemchipkarten und HSMs für die Wurzelzertifizierungsstelle und die Mitarbeiter-CAs der RV-Träger und erstellt die zugehörigen Zertifikate.

Bis zum 23.01.2009 wurden für qualifizierte CAs ebenso CRL-Signer-Zertifikate erstellt.

Die Personalisierung findet mit Hilfe der zentralen Trustcenter-Systeme statt. Die Zertifikate werden während des Prozesses ebenfalls mit Hilfe der zentralen Trustcenter-Systeme erzeugt.

Das Aufsetzen der Wurzel- und Mitarbeiter-CAs sowie der jährliche Schlüsselwechsel werden protokolliert (mindestens Datum, beteiligte Systemverwalter, Inhaber der Systemchipkarte, Pseudonyme, RV-Träger). Alle Protokolle werden im Archiv der Wurzelzertifizierungsstelle aufbewahrt. Für die Anfertigung der Protokolle ist der Leiter der Wurzelzertifizierungsstelle verantwortlich.

Mit Abschluss der Key-Ceremony sind die ausgestellten Schlüssel und Zertifikate betriebsbereit.

2.1.3 Sperrung

Alle durch die Wurzelzertifizierungsstelle ausgestellten Zertifikate werden auf Antrag eines Sperrberechtigten durch zwei Systemverwalter gesperrt.

In § 8 SigG sind die Sperrberechtigten für qualifizierte Zertifikate benannt. Für die Wurzelzertifizierungsstelle kommen folgende in Betracht:

- die Bundesnetzagentur,
- die Deutsche Rentenversicherung Bund als Betreiber der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung,
- der RV-Träger als Betreiber einer Zertifizierungsstelle des RV-Trägers für die Mitarbeiter-CA-Zertifikate.

Im fortgeschrittenen Bereich entfällt die Bundesnetzagentur als Sperrberechtigte.

Die Signaturschlüssel-Inhaber haben gegenüber der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung auf ihr Recht zur Sperrung verzichtet.

Sperrgründe sind:

- Schließung des Betriebs (cessationOfOperation),
- Root-CA-Schlüssel kompromittiert (cACompromise),
- CA-Schlüssel kompromittiert (cACompromise),
- Ein ausgestelltes Zertifikat enthält unrichtige Angaben,
- Der ZDA Deutsche Rentenversicherung Bund stellt seine Tätigkeit ein und kein anderer ZDA übernimmt die Zertifikate,
- Systemchipkarte nicht funktionsfähig,
- Verdacht der unbefugten Nutzung (keyCompromise).
- Sperrgrund unbekannt (unspecified).

2.1.4 Schlüsselerneuerung

Die Key-Ceremony wird jährlich wiederholt. Die Zertifikate der Wurzelzertifizierungsstelle werden für 5 Jahre ausgestellt, die Zertifikate der Antragsteller (Mitarbeiter-CAs) auf 4 Jahre.

Neue CA-Zertifikate werden außerdem erstellt, wenn der Signaturschlüssel-Inhaber nicht mehr in der Lage ist, die PIN einzugeben (zum Beispiel Ausscheiden, Tod).

Das alte Schlüsselmaterial wird unbrauchbar gemacht, ohne die zugehörigen Zertifikate zu sperren.

2.1.5 Archivierung

Jeder Zertifizierungsdiensteanbieter unterliegt einer im Signaturgesetz und in der Signaturverordnung geregelten Dokumentations- und Aufbewahrungspflicht („Archivierung“).

Der Mitarbeiter Archivierung ist für die Entgegennahme, für das ordnungsgemäße Einsortieren sowie für das auf Anfrage erfolgende Heraussuchen der Papierdokumente verantwortlich. Laut Signaturgesetz ist dem Signaturschlüssel-Inhaber auf Verlangen Einsicht in die ihn betreffenden Daten und Verfahrensschritte zu gewähren.

Die bei der Durchführung der Prozesse anfallenden Protokolle und gegebenenfalls weitere anfallende Dokumente werden von den zuständigen Rolleninhabern an das Archiv weitergeleitet.

2.2 OCSP-Signer-Zertifikate für Wurzel- und Mitarbeiter-CAs

2.2.1 Registrierung

Folgende Signaturschlüsselinhaber werden in der Wurzelzertifizierungsstelle durch den Leiter der Wurzelzertifizierungsstelle identifiziert:

- Rolleninhaber Systemverwalter Server 1 am Standort des aktiven Systems
- Rolleninhaber Systemverwalter Server 1 am Standort des Backup-Systems

Der Leiter der Wurzelzertifizierungsstelle der DRV erhebt folgende personenbezogene Daten aus dem Personalausweis bzw. Reisepass und trägt sie in das Protokoll Betriebsaufnahme bzw. Schlüsselwechsel ein:

- Name
- Vorname
- Geburtsdatum
- Geburtsort
- Staatsangehörigkeit

Der Leiter der Wurzelzertifizierungsstelle der DRV erhebt die Personenkennziffer aus dem Dienstausweis und trägt sie in das Protokoll Betriebsaufnahme bzw. Schlüsselwechsel ein. Das Pseudonym wird spezifiziert und im Protokoll vermerkt.

Die Signaturschlüsselinhaber unterzeichnen eine vertragliche Vereinbarung mit der Deutschen Rentenversicherung Bund bzw. dem jeweiligen RV-Träger, dass sie auf die Sperrung der OCSP-Signer-Zertifikate verzichten und dem öffentlichen Abruf der OCSP-Signer-Zertifikate zustimmen. Sie werden in der gleichen Vereinbarung von der Haftung durch Missbrauch der Systemschlüssel freigestellt.

2.2.2 Key-Ceremony

Alle OCSP-Signer-Schlüssel der qualifizierten CAs werden auf sicheren Signaturerstellungseinheiten (Systemchipkarten) betrieben. Alle OCSP-Signer-Schlüssel der fortgeschrittenen CAs werden auf HSMs betrieben, deren Sicherheit sich an den Vorgaben des Signaturgesetzes orientiert.

Die Wurzelzertifizierungsstelle der Deutschen Rentenversicherung personalisiert bei der Betriebsaufnahme, im Rahmen der Schlüsselerneuerung und bei notwendigen Ersatzleistungen Systemchipkarten und HSMs für die OCSP-Signer der Wurzelzertifizierungsstelle und der Mitarbeiter-CAs der RV-Träger.

Die Personalisierung findet mit Hilfe der zentralen Trustcenter-Systeme statt. Die Zertifikate werden während des Prozesses ebenfalls mit Hilfe der zentralen Trustcenter-Systeme erzeugt.

Die Key-Ceremony wird protokolliert (mindestens Datum, beteiligte Systemverwalter, Inhaber der Systemchipkarte, Pseudonyme, RV-Träger). Alle Protokolle werden im Archiv der Wurzelzertifizierungsstelle aufbewahrt. Für die Anfertigung der Protokolle ist der Leiter der Wurzelzertifizierungsstelle verantwortlich.

Mit Abschluss der Key-Ceremony sind die ausgestellten Schlüssel und Zertifikate betriebsbereit.

2.2.3 Sperrung

- Die Sperrung entspricht Kap. 2.1.3

2.2.4 Schlüsselerneuerung

Die Key-Ceremony für OCSP-Signer-Zertifikate der Root-CAs und der Mitarbeiter-CAs wurde bis zum Jahr 2010 jährlich wiederholt. Ab dem Jahr 2011 wird die Key-Ceremony für OCSP-Signer-Zertifikate nicht mehr jährlich durchgeführt, sondern rechtzeitig vor Ablauf ihrer Gültigkeit.

Neue OCSP-Signer-Zertifikate werden außerdem erstellt, wenn der Signaturschlüssel-Inhaber nicht mehr in der Lage ist, die PIN einzugeben (zum Beispiel Ausscheiden, Tod).

Die OCSP-Signer-Zertifikate werden so ausgestellt, dass deren Gültigkeit vor dem Auslaufen des Zertifikates der ausstellenden CA endet.

Das alte Schlüsselmaterial wird unbrauchbar gemacht, ohne die zugehörigen Zertifikate zu sperren.

2.2.5 Archivierung

Die Archivierung erfolgt gemäß den Regelungen des Abschnitts 2.1.5 auch für die bei der Erstellung, Erneuerung und Sperrung von OCSP-Signer-Zertifikaten und -schlüsseln anfallenden Unterlagen und Daten.

2.3 TSP-Signer-Zertifikate

2.3.1 Registrierung

Folgende Signaturschlüsselinhaber werden in der Wurzelzertifizierungsstelle durch den Leiter der Wurzelzertifizierungsstelle identifiziert:

- Rolleninhaber Systemverwalter Server 1 am Standort des aktiven Systems
- Rolleninhaber Systemverwalter Server 1 am Standort des Backup-Systems

Der Leiter der Wurzelzertifizierungsstelle der DRV erhebt folgende personenbezogene Daten aus dem Personalausweis bzw. Reisepass und trägt sie in das Protokoll Betriebsaufnahme des Zeitstempeldienstes ein:

- Name
- Vorname
- Geburtsdatum
- Geburtsort
- Staatsangehörigkeit

Der Leiter der Wurzelzertifizierungsstelle der DRV erhebt die Personenkennziffer aus dem Dienstausweis und trägt sie in das Protokoll Betriebsaufnahme bzw. Schlüsselwechsel des Zeitstempeldienstes ein. Das Pseudonym wird spezifiziert und im Protokoll vermerkt.

Die Signaturschlüsselinhaber unterzeichnen eine vertragliche Vereinbarung mit der Deutschen Rentenversicherung Bund, dass sie auf die Sperrung der TSP-Signer-Zertifikate verzichten und dem öffentlichen Abruf der TSP-Signer-Zertifikate zustimmen. Sie werden in der gleichen Vereinbarung von der Haftung durch Missbrauch der TSP-Systemchipkarte freigestellt.

2.3.2 Key-Ceremony

Der Zeitstempeldienst verwendet sichere Signaturerstellungseinheiten, die nach Signaturgesetz geprüft und bestätigt sind. Die sichere Schlüsselerzeugung erfolgt unter Beachtung der Bestätigungsauflagen.

Die Wurzelzertifizierungsstelle der Deutschen Rentenversicherung personalisiert bei der Betriebsaufnahme, im Rahmen der Schlüsselerneuerung und bei notwendigen Ersatzleistungen Systemchipkarten für TSP-Signer.

Die Personalisierung findet mit Hilfe der zentralen Trustcenter-Systeme statt. Die Zertifikate werden während des Prozesses ebenfalls mit Hilfe der zentralen Trustcenter-Systeme erzeugt.

Das Personalisieren der TSP-Signaturerstellunseinheiten wird im Protokoll Betriebsaufnahme bzw. Schlüsselwechsel des Zeitstempeldienstes vermerkt (mindestens Datum, beteiligte Systemverwalter, Inhaber der Systemchipkarten, Pseudonyme). Das Protokoll wird im Archiv der Wurzelzertifizierungsstelle aufbewahrt. Für die Anfertigung der Protokolle ist der Leiter der Wurzelzertifizierungsstelle verantwortlich.

Mit Abschluss der Key-Ceremony sind die ausgestellten Schlüssel und Zertifikate betriebsbereit.

2.3.3 Sperrung

Die Sperrung von TSP-Signer-Zertifikaten erfolgt gemäß Abschnitt 2.1.3.

Sperrgründe sind abweichend von der Regelung im oben genannten Abschnitt:

- Schließung des Betriebs (cessationOfOperation),
- Root-CA-Schlüssel kompromittiert (cACompromise),
- Ein ausgestelltes Zertifikat enthält unrichtige Angaben,
- Der ZDA Deutsche Rentenversicherung Bund stellt seine Tätigkeit ein und kein anderer ZDA übernimmt die Zertifikate,
- Systemchipkarte nicht funktionsfähig,
- Verdacht der unbefugten Nutzung (keyCompromise).
- Sperrgrund unbekannt (unspecified).

2.3.4 Schlüsselerneuerung

Die Key-Ceremony für TSP-Signer-Zertifikate wurde bis zum Jahr 2010 jährlich wiederholt. Ab dem Jahr 2011 wird die Key-Ceremony für TSP-Signer-Zertifikate nicht mehr jährlich durchgeführt, sondern rechtzeitig vor Ablauf ihrer Gültigkeit.

Die TSP-Signer-Zertifikate werden so ausgestellt, dass deren Gültigkeit vor dem Auslaufen des Zertifikates der ausstellenden qualifizierten Root-CA endet.

Neue TSP-Signer-Zertifikate werden außerdem erstellt, wenn der Signaturschlüssel-Inhaber nicht mehr in der Lage ist, die PIN einzugeben (zum Beispiel Ausscheiden, Tod).

Das alte Schlüsselmaterial wird unbrauchbar gemacht, ohne die zugehörigen Zertifikate zu sperren.

2.3.5 Archivierung

Die Archivierung erfolgt gemäß den Regelungen des Abschnitts 2.1.5 auch für die bei der Erstellung, Erneuerung und Sperrung von TSP-Signer-Zertifikaten und -schlüsseln anfallenden Unterlagen und Daten.

2.4 CA-Zertifikate für Server-CAs

2.4.1 Registrierung

Zertifikatsinhaber für die Zertifikate der Server-CAs ist der Leiter der Wurzelzertifizierungsstelle.

Der Sicherheitsbeauftragte der Deutschen Rentenversicherung Bund identifiziert den Leiter der Wurzelzertifizierungsstelle und erhebt folgende personenbezogene Daten aus dem Personalausweis bzw. Reisepass und trägt sie in das Protokoll Betriebsaufnahme ein:

- Name
- Vorname
- Geburtsdatum
- Geburtsort
- Staatsangehörigkeit

Der Sicherheitsbeauftragte der Deutschen Rentenversicherung Bund erhebt die Personenkennziffer aus dem Dienstausweis und trägt sie in das Protokoll Betriebsaufnahme bzw. Schlüsselwechsel ein.

Der Leiter der Wurzelzertifizierungsstelle unterzeichnet eine vertragliche Vereinbarung, dass er auf die Sperrung der Systemzertifikate verzichtet und dem öffentlichen Abruf der Systemzertifikate zustimmt. Er wird in der gleichen Vereinbarung von der Haftung durch Missbrauch der Systemschlüssel freigestellt.

2.4.2 Key-Ceremony

Die CA-Signer-Schlüssel der Server-CAs werden auf HSMs betrieben, deren Sicherheit sich an den Vorgaben des Signaturgesetzes orientiert.

Die Wurzelzertifizierungsstelle der Deutschen Rentenversicherung erzeugt bei der Betriebsaufnahme und bei Schlüsselerneuerung sowie bei notwendigen Ersatzleistungen Schlüssel und Zertifikate für die Server-CAs.

Die Erzeugung des Schlüsselmaterials und der Zertifikate findet mit Hilfe der zentralen Trustcenter-Systeme statt.

Das Aufsetzen der Server-CAs sowie ein Schlüsselwechsel werden protokolliert (mindestens Datum, beteiligte Systemverwalter, Schlüssel-Inhaber). Alle Protokolle werden im Archiv der Wurzelzertifizierungsstelle aufbewahrt. Für die Anfertigung der Protokolle ist der Leiter der Wurzelzertifizierungsstelle verantwortlich.

Mit Abschluss der Key-Ceremony sind die ausgestellten Schlüssel und Zertifikate betriebsbereit.

2.4.3 Sperrung

Alle durch die Wurzelzertifizierungsstelle ausgestellten Server-CA-Zertifikate werden auf Antrag eines Sperrberechtigten durch zwei Systemverwalter gesperrt.

Für die Wurzelzertifizierungsstelle kommen folgende Sperrberechtigte in Betracht:

- die Deutsche Rentenversicherung Bund als Betreiber der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung,
- die Deutsche Rentenversicherung Bund als Betreiber der Server-CAs.

Die Schlüssel-Inhaber haben gegenüber der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung auf ihr Recht zur Sperrung verzichtet.

Sperrgründe sind:

- Schließung des Betriebs (cessationOfOperation),
- Root-CA-Schlüssel kompromittiert (cACompromise),
- CA-Schlüssel kompromittiert (cACompromise),
- Ein ausgestelltes Zertifikat enthält unrichtige Angaben,

- Der ZDA Deutsche Rentenversicherung Bund stellt seine Tätigkeit ein und kein anderer ZDA übernimmt die Zertifikate,
- Systemschlüssel wegen defektem Schlüsselträger nicht funktionsfähig,
- Verdacht der unbefugten Nutzung (keyCompromise).
- Sperrgrund unbekannt (unspecified).

2.4.4 Schlüsselerneuerung

Für die NQ DRV CA wird die Key-Ceremony jährlich wiederholt.

Für die NQ DRV WAN01 CA erfolgt eine Key-Ceremony nur in Abstimmung mit dem Teilnehmerkreis.

Die Zertifikate der Server-CAs werden auf 4 Jahre ausgestellt.

Neue Server-CA-Zertifikate werden außerdem erstellt, wenn der Schlüssel-Inhaber nicht mehr in der Lage ist, die PIN einzugeben (zum Beispiel Ausscheiden, Tod).

Das alte Schlüsselmaterial wird unbrauchbar gemacht, ohne die zugehörigen Zertifikate zu sperren.

2.4.5 Archivierung

Der Mitarbeiter Archivierung ist für die Entgegennahme, für das ordnungsgemäße Einsortieren sowie für das auf Anfrage erfolgende Heraussuchen der Papierdokumente verantwortlich. Dem Schlüssel-Inhaber wird auf Verlangen Einsicht in die ihn betreffenden Daten und Verfahrensschritte gewährt.

Die bei der Durchführung der Prozesse anfallenden Protokolle und gegebenenfalls weitere anfallende Dokumente werden von den zuständigen Rolleninhabern an das Archiv weitergeleitet.

2.5 OCSP-Signer-Zertifikate der Server-CAs

Für die von der NQ DRV CA ausgestellten Zertifikate werden OCSP-Auskünfte erteilt.

Für die von der NQ DRV WAN01 CA ausgestellten Zertifikate werden keine OCSP-Auskünfte erteilt.

2.5.1 Registrierung

Folgende Signaturschlüsselinhaber werden in der Wurzelzertifizierungsstelle durch den Leiter der Wurzelzertifizierungsstelle identifiziert:

- Rolleninhaber Systemverwalter Server 1 am Standort des aktiven Systems
- Rolleninhaber Systemverwalter Server 1 am Standort des Backup-Systems

Der Leiter der Wurzelzertifizierungsstelle der DRV erhebt folgende personenbezogene Daten aus dem Personalausweis bzw. Reisepass und trägt sie in das Protokoll Betriebsaufnahme bzw. Schlüsselwechsel ein:

- Name
- Vorname
- Geburtsdatum
- Geburtsort
- Staatsangehörigkeit

Der Leiter der Wurzelzertifizierungsstelle der DRV erhebt die Personenkennziffer aus dem Dienstausweis und trägt sie in das Protokoll Betriebsaufnahme bzw. Schlüsselwechsel ein.

Die Signaturschlüsselinhaber unterzeichnen eine vertragliche Vereinbarung mit der Deutschen Rentenversicherung Bund, dass sie auf die Sperrung der OCSP-Signer-Zertifikate verzichten und dem öffentlichen Abruf der OCSP-Signer-Zertifikate zustimmen. Sie werden in der gleichen Vereinbarung von der Haftung durch Missbrauch der Systemschlüssel freigestellt.

2.5.2 Key-Ceremony

Die OCSP-Signer-Schlüssel werden auf HSMs betrieben, deren Sicherheit sich an den Vorgaben des Signaturgesetzes orientiert.

Die Wurzelzertifizierungsstelle der Deutschen Rentenversicherung erzeugt bei der Betriebsaufnahme und bei Schlüsselerneuerung sowie bei notwendigen Ersatzleistungen Schlüssel und Zertifikate für OCSP-Signer.

Die Erzeugung des Schlüsselmaterials und der Zertifikate findet mit Hilfe der zentralen Trustcenter-Systeme statt.

Die Key-Ceremony wird protokolliert (mindestens Datum, beteiligte Systemverwalter, Schlüssel-Inhaber). Alle Protokolle werden im Archiv der Wurzelzertifizierungsstelle aufbewahrt. Für die Anfertigung der Protokolle ist der Leiter der Wurzelzertifizierungsstelle verantwortlich.

Mit Abschluss der Key-Ceremony sind die ausgestellten Schlüssel und Zertifikate betriebsbereit.

2.5.3 Sperrung

- Die Sperrung entspricht Kap. 2.4.3.

2.5.4 Schlüsselerneuerung

Die Key-Ceremony für OCSP-Signer-Zertifikate wird rechtzeitig vor Ablauf ihrer Gültigkeit durchgeführt.

Neue OCSP-Signer-Zertifikate werden außerdem erstellt, wenn der Schlüssel-Inhaber nicht mehr in der Lage ist, die PIN einzugeben (zum Beispiel Ausscheiden, Tod).

Die OCSP-Signer-Zertifikate werden so ausgestellt, dass deren Gültigkeit vor dem Auslaufen des Zertifikates der ausstellenden Server-CA endet.

Das alte Schlüsselmaterial wird unbrauchbar gemacht, ohne die zugehörigen Zertifikate zu sperren.

2.5.5 Archivierung

Die Archivierung erfolgt gemäß den Regelungen des Abschnitts 2.4.5.

3 Ausführende Rollen

Die Prozesse der Wurzelzertifizierungsstellen werden von den in der Tabelle 1 genannten Rolleninhabern ausgeführt:

Tabelle 1: Administrative Rollen und ihre Aufgaben

Administrative Rollen	Aufgaben
Leiter der Wurzelzertifizierungsstelle	Der Leiter der Wurzelzertifizierungsstelle verantwortet den Betrieb und die Zertifizierungstätigkeit der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung. Diese Rolle umfasst dazu die Leitung aller Prozesse des Zertifizierungsdienstes und den Bericht an die Geschäftsführung der Deutschen Rentenversicherung Bund.
Leiter der Zertifizierungsstelle	Der Leiter der Zertifizierungsstelle verantwortet die Leitung aller Prozesse der Zertifizierungsdienste des jeweiligen RV-Trägers und die Abstimmung mit dem Leiter der Wurzelzertifizierungsstelle. Er berichtet an seine Geschäftsführung.
Sicherheitsbeauftragter	Der Sicherheitsbeauftragte ist für die Sicherheit des ZDA und in diesem Zusammenhang insbesondere für die Sicherstellung der allgemeinen Sicherheit, des Gebäudeschutzes und des Brandschutzes verantwortlich.
Sicherheitsbeauftragter des Rechenzentrums	Der Sicherheitsbeauftragte des Rechenzentrums veranlasst die Einrichtung von Sicherheitsbereichen im Rechenzentrum und vergibt bzw. storniert Zutrittsberechtigungen. Der Sicherheitsbeauftragte des Rechenzentrums arbeitet unter anderem mit dem Sicherheitsbeauftragten zusammen.
IT-Sicherheitsbeauftragter	Der IT-Sicherheitsbeauftragte verantwortet die IT-Sicherheit beim Betrieb der (Wurzel-) Zertifizierungsstelle. Die Hauptaufgabe des IT-Sicherheitsbeauftragten besteht darin, die Leitung der (Wurzel-) Zertifizierungsstelle bei der Wahrnehmung ihrer Aufgaben bezüglich der IT-Sicherheit zu beraten und bei deren Umsetzung zu unterstützen. Für die Zertifizierungsdienste hat der IT-Sicherheitsbeauftragte dafür zu sorgen, dass der Betrieb entsprechend den Sicherheitsbestimmungen durchgeführt wird.
Datenschutzbeauftragter	Der Datenschutzbeauftragte hat die Aufgabe, die Ausführung der Vorschriften der jeweiligen Datenschutzgesetze bei der Aufgabenerledigung sicherzustellen.
Revision	Die Revision ist zuständig für die Kontrolle und Überprüfung der ordnungsgemäßen Umsetzung des Sicherheitskonzepts und des Organisationskonzepts.

Administrative Rollen	Aufgaben
Kryptomanager	Der Kryptomanager ist für die Betreuung der kryptographischen Verfahren zuständig. Dazu gehört die Verantwortung für die kryptographische Sicherheit der in der Wurzelzertifizierungsstelle sowie in der Zertifizierungsstelle des RV-Trägers eingesetzten kryptographischen Algorithmen. Hierfür ist eine ständige Verfolgung der im Bundesanzeiger durch die Bundesnetzagentur veröffentlichten Einschätzungen bzgl. der Eignung der kryptographischen Algorithmen notwendig.
Leiter Personalisierung	Der Leiter Personalisierung verantwortet die ordnungsgemäße Durchführung und Dokumentation des Personalisierungsprozesses und die Verwaltung der dafür erforderlichen Mitarbeiterchipkarten nach den Vorgaben des Sicherheitskonzepts.
Leiter Systemverwaltung	Der Leiter Systemverwaltung ist für die Personalauswahl und die Personalplanung für die Systemverwalter Server und die Systemverwalter Netzwerk zuständig.
Systemverwalter Server (1+2)	Der Systemverwalter Server 1 ist gemeinsam mit dem Systemverwalter Server 2 für die Initialisierung und die Konfiguration der Server zuständig. Der Systemverwalter Server 2 überwacht insbesondere die Tätigkeiten des Systemverwalters Server 1 und bestätigt durch seine Unterschrift auf dem Administrationsprotokoll die Korrektheit gegebenenfalls vorgenommener Änderungen. Es ist eine ständige Rufbereitschaft von mindestens zwei Systemverwaltern Server erforderlich.
Systemverwalter Netzwerk (1+2)	Der Systemverwalter Netzwerk 1 ist zusammen mit dem Systemverwalter Netzwerk 2 für alle im Netzwerk anfallenden administrativen Aufgaben zuständig. Der Systemverwalter Netzwerk 2 überwacht insbesondere die Tätigkeiten des Systemverwalters Netzwerk 1 und bestätigt durch seine Unterschrift auf dem Administrationsprotokoll die Korrektheit gegebenenfalls vorgenommener Änderungen. Es ist eine ständige Rufbereitschaft von mindestens zwei Systemverwaltern Netzwerk erforderlich.

4 Bekanntmachung und Verzeichnisdienst

4.1 Verzeichnisdienst

Die von der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung ausgestellten Zertifikate (einschl. TSP-Signer- und OCSP-Signer-Zertifikate sowie bis zum 23.01.2009 verwendete CRL-Signer-Zertifikate) werden in den Verzeichnisdiensten der Deutschen Rentenversicherung Bund für mindestens 30 Jahre nach dem Ablauf der Gültigkeit nachprüfbar gehalten bzw. zum Abruf bereitgestellt. Verzeichnisdienstauskünfte werden für alle Zertifikatsarten (qualifizierte Zertifikate, weitere Schlüsselzertifikate) in gleicher Weise erteilt. D. h. es werden die vom Signaturgesetz geforderten Auskünfte auch für fortgeschrittene Zertifikate erteilt (Ausnahme: NQ DRV WAN01 CA – siehe Abschnitt 2.5). Zertifikate enthalten die Dienstadressen für den Abruf von CA-Zertifikaten, Sperrlisten und OCSP-Statusauskünften. Seit dem 23.01.2009 werden für qualifizierte CAs bis auf Weiteres keine Sperrlisten (CRLs und Delta-CRLs) mehr bereitgestellt.
Der Verzeichnisdienst besteht aus 2 Komponenten:

1. LDAP-Verzeichnisdienst
2. OCSP-Responder

Die Grundlage für die technische Spezifikation der Komponenten des Verzeichnisdienstes deckt den ISIS-MTT-Standard in der Version 1.0.2 ab. Die Anforderungen des SigG sind in diesem Standard berücksichtigt. Folgende Teile des ISIS-MTT Standards sind für den Verzeichnisdienst berücksichtigt:

- Part 1: Certificate and CRL Profiles — Format für Zertifikate und Sperrlisten
- Part 4: Operational Protocols — LDAP, OCSP und Zeitstempel

4.1.1 LDAP-Verzeichnisdienst

Der LDAP-Verzeichnisdienst hält CA-Zertifikate, OCSP-Signer-Zertifikate, bis zum 23.01.2009 verwendete CRL-Signer-Zertifikate, TSP-Signer-Zertifikate sowie Sperrlisten für fortgeschrittene CAs abrufbar. Die Sperrlisten enthalten Seriennummern und das Sperrdatum relevanter Zertifikate.

Alle Informationen des LDAP-Verzeichnisdienstes sind über http und LDAP abfragbar. Die Adresse des LDAP- und http-Dienstes für CA-Zertifikate ist in der Extension „IssuerAltNames“ angegeben. Die Adressen des LDAP- und http-Dienstes für Sperrlisten der fortgeschrittenen CAs sind in den Zertifikaten als CRL-DistributionPoints angegeben.

Jede fortgeschrittene CA führt genau eine Sperrliste über die ihrerseits ausgestellten Zertifikate als X.509 CRL Version 2 Liste ohne optionale Erweiterungen im Verzeichnisdienst. Außerdem werden für fortgeschrittene CAs Delta-CRLs generiert, die bei jeder Sperrung neu erzeugt werden und die jeweils aktuellste Gesamtsperrliste um die Zertifikate ergänzen, die seit der Veröffentlichung der Gesamtsperrliste hinzugekommen sind. Die Adressen der Delta-CRLs können der Extension „freshest CRL“ der jeweiligen Gesamtsperrliste entnommen werden.

CRLs und Delta-CRLs der fortgeschrittenen CAs werden mit dem CA-Schlüssel signiert. Die bis zum 23.01.2009 für qualifizierte CAs erzeugten CRLs und Delta-CRLs wurden mit einem separaten CRL-Signer-Schlüssel signiert.

4.1.2 OCSP-Responder

Der Status der CA-Zertifikate und TSP-Signer-Zertifikate kann über OCSP abgefragt werden (Ausnahme: NQ DRV WAN01 CA – siehe Abschnitt 2.5). Über den OCSP-Responder werden Vorhandenseins- und Sperrauskünfte erteilt. Die notwendigen Informationen für den Zugriff auf den Auskunftsdienst sind in den CA-Zertifikaten und TSP-Signer-Zertifikaten im Feld „AuthorityInfoAccess“ angegeben. Die OCSP-Zertifikate, mit welchen die Auskünfte signiert werden, sind wie andere Zertifikate im zentralen Verzeichnisdienst abgelegt.

Der Auskunftsdienst für den qualifizierten Bereich genügt den Sicherheitsanforderungen des SigG (§17 Abs. 3 Nr. 2) mit der Stufe „ITSEC E2 hoch“. Die Signaturerstellungseinheit des Verzeichnisdienstes genügt den Sicherheitsanforderungen des SigG gemäß §17 Abs. 1 SigG mindestens mit der Stufe „ITSEC E3 hoch“.

Im fortgeschrittenen Bereich werden vertrauenswürdige Systeme verwendet, die mit Ausnahme der Produkte zur Generierung und Speicherung der Schlüssel den Vorgaben des deutschen Signaturgesetzes und der Signaturverordnung entsprechen. Die Sicherheit der Schlüssel wird durch flankierende Maßnahmen sichergestellt.

4.2 Veröffentlichung von Informationen der PKI-Instanzen

Das vorliegende Dokument wird auf der Web-Seite der Deutschen Rentenversicherung Bund

http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html

veröffentlicht.

Zertifikate der Wurzelzertifizierungsstellen werden auf der Web-Seite der Deutschen Rentenversicherung Bund und in der Zeitschrift „RVaktuell“, dem amtlichen Veröffentlichungsblatt der Deutschen Rentenversicherung Bund, veröffentlicht. Außerdem werden sie zum elektronischen Download angeboten und im Verzeichnisdienst veröffentlicht.

4.3 Häufigkeit und Zyklen für Veröffentlichungen

- Die Veröffentlichung der vorliegenden CPS und der CP erfolgt jeweils unmittelbar nach Erstellung bzw. Aktualisierung des Dokumentes.
- Die Veröffentlichung der Zertifikate erfolgt unmittelbar nach Aktivierung des betreffenden Zertifikates bzw. nach Erneuerung.
- Die Veröffentlichung von Statusinformationen erfolgt unmittelbar nach Erstellung des betreffenden Zertifikates bzw. nach Änderung des Zertifikatsstatus.
- Gesamt-Sperrlisten für die fortgeschrittenen Wurzel-CA werden alle 4 Tage erneuert und veröffentlicht. Sie sind für 1 Woche gültig.
- Sobald Sperrungen für fortgeschrittene Zertifikate umgesetzt sind, werden Delta-CRLs im Verzeichnisdienst eingestellt.

5 Namenskonzept

Die beiden CAs der Wurzel und die ausgestellten CA-Zertifikate werden in den Zertifikaten ISIS-MTT-konform mit den DN-Attributen

- OrganizationalUnit
- Organization
- Country

benannt. Gemäß SigG wird mit „Organization“ und „Country“ der Zertifizierungsdienstanbieter bezeichnet, der bei der Bundesnetzagentur in der Betriebsanzeige als Betreiber genannt ist. Mit „Organizational Unit“ werden die verschiedenen CAs eines RV-Trägers voneinander unterschieden.

Die für die Wurzel-CAs verwendeten Namen sind in Tabelle 2 dargestellt.

Tabelle 2: Namen der Wurzel-CAs

Wurzelzertifizierungsstelle für qualifizierte Zertifikate	„OU=QC Root CA, O=Deutsche Rentenversicherung, C=DE“
Wurzelzertifizierungsstelle für sonstige Zertifikate	„OU=NQ Root CA, O= Deutsche Rentenversicherung, C=DE“

OCSP-Signer-Zertifikate werden auf den Namen der zugehörigen CA ausgestellt und erhalten zusätzlich ein CN-Attribut (zum Beispiel QC Root OCSP bzw. NQ Root OCSP).

TSP-Signer-Zertifikate erhalten den Namen der QC Root CA und zusätzlich ein CN-Attribut (QC Root TSP).

Die bis zum 23.01.2009 im qualifizierten Bereich verwendeten CRL-Signer-Zertifikate wurden auf den Namen der zugehörigen CA ausgestellt und enthielten kein zusätzliches CN-Attribut.

5.1 Eindeutigkeit von Namen

Die Eindeutigkeit der Namen ergibt sich aus der Eindeutigkeit der Organisationsbezeichnungen.

5.2 Anonymität und Pseudonyme für Zertifikatseigentümer

CA-Zertifikate, OCSP-Signer-Zertifikate und bis zum 23.01.2009 verwendete CRL-Signer-Zertifikate haben fest vorgegebene Namen. Die Namen der qualifizierten CA-Zertifikate, der qualifizierten OCSP-Signer-Zertifikate und der TSP-Signer-Zertifikate stellen Pseudonyme im Sinne des SigG dar, sind entsprechend gekennzeichnet, unverwechselbar und lassen die Identifikation einer natürlichen Person zu, die den Einsatz der zugehörigen Schlüssel verantwortet.

Weitere Details zur Namensgebung sind dem Anhang Zertifikatsprofile zu entnehmen.

6 Prüfung des Zertifikatsstatus durch Dritte

Zur vollständigen Prüfung des Zertifikatsstatus müssen Zertifikatsketten gebildet und ihre Signaturen geprüft werden, bis eine Zertifikatskette mit korrekten Signaturen auf einem von der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung herausgegebenen Wurzelzertifikat endet und keine in den Zertifikaten enthaltene kritische Erweiterung die Kette ungültig macht. Weiterhin darf kein Zertifikat zum für seine Prüfung relevanten Zeitpunkt ungültig oder gesperrt sein. Die Wahl des relevanten Zeitpunkts für die Prüfung der Gültigkeit eines Zertifikats erfolgt nach dem Kettenmodell. Danach ist der zur Prüfung eines Signaturzertifikats relevante Zeitpunkt der Zeitpunkt, an dem die mit dem Zertifikat zu prüfende Signatur geleistet wurde. Bei Verschlüsselungs- und Authentifizierungszertifikaten ist der relevante Zeitpunkt der aktuelle Zeitpunkt. Die Gültigkeitszeiträume der Zertifikate sind so strukturiert, dass eine Prüfung gemäß RFC zu korrekten Gültigkeitsaussagen führt, mit der Ausnahme des Falls einer Sperrung des Zertifikats einer Zertifizierungsstelle. In diesem Fall liefert nur die Gültigkeitsprüfung nach Kettenmodell die korrekte Gültigkeitsaussage.

Eine Prüfung des Zertifikatsstatus qualifizierter Zertifikate durch einen Dritten muss immer über OCSP-Anfrage erfolgen.

Eine Prüfung des Zertifikatsstatus fortgeschrittener Zertifikate kann darüber hinaus auch gegen Sperrlisten erfolgen.

Eine Ausnahme stellt die NQ DRV WAN01 CA dar: hier ist eine Prüfung ausschließlich gegen Sperrlisten möglich, siehe auch Abschnitt 2.5.

Das Vertrauen auf die Richtigkeit unvollständig geprüfter Zertifikate geschieht auf eigenes Risiko des Prüfers.

7 Sicherheitsmaßnahmen

7.1 Sicherheitsziele

Der Betrieb einer Zertifizierungsstelle unterliegt hohen Sicherheitsanforderungen. Die dafür zu treffenden Maßnahmen dienen insbesondere den folgenden Sicherheitszielen:

- **Vertraulichkeit**
  Die Kenntnisnahme schützenswerter Daten durch Unbefugte muss wirksam ausgeschlossen werden. Dies betrifft insbesondere kryptographische Geheimnisse (private Schlüssel), PINs und personenbezogene Daten der Karteninhaber.
- **Integrität**
  Daten müssen bei ihrer Speicherung und Übertragung vor einer Veränderung, Löschung oder Erweiterung durch Unbefugte geschützt werden. Dies betrifft insbesondere die in den Zertifikaten und Sperrlisten enthaltenen Daten, die im IT-System Verzeichnis bereitgehalten werden und die Registrierungsdaten, die die Grundlage für die Ausstellung von Zertifikaten bilden.
- **Verfügbarkeit**
  Systeme und Daten müssen ausreichend verfügbar sein, um ihren jeweiligen Zweck geeignet zu erfüllen. Besonders hohe Verfügbarkeitsanforderungen ergeben sich dabei an das IT-System Verzeichnis, das für die Gültigkeitsprüfung von Zertifikaten erforderlich ist, und das IT-System Sperrdienst.
- **Nachvollziehbarkeit**
  Die gesamte Zertifizierungstätigkeit muss revisionssicher dokumentiert sein, damit in Zweifelsfällen die erforderliche Nachvollziehbarkeit gegeben ist. Dies umfasst die Nachvollziehbarkeit der Prozesse anhand entsprechender Papierbelege ebenso wie die elektronische Protokollierung der Prozesse durch die IT-Systeme.

Die Wurzelzertifizierungsstelle der Deutschen Rentenversicherung arbeitet nach einem Sicherheitskonzept, das die Anforderungen des SigG erfüllt.

7.2 Gesetzliche Anforderungen

Bei der Bestimmung des erforderlichen Schutzniveaus sind die besonderen gesetzlichen Anforderungen zu berücksichtigen, die sich für einen Zertifizierungsdiensteanbieter, der qualifizierte elektronische Zertifikate ausstellt, aus SigG und SigV ergeben. SigG und SigV definieren den einzuhaltenden Sicherheitsstandard.

Darüber hinaus sind für die Bearbeitung personenbezogener Daten die Vorgaben der Datenschutzgesetzgebung zu beachten.

7.3 Personelle Sicherheitsmaßnahmen

Nach § 4 Abs.2 SigG hat ein ZDA zuverlässiges und qualifiziertes Personal einzusetzen. Daher ist die Zuverlässigkeit der Mitarbeiter des ZDA sicherzustellen – sowohl bei der Neueinstellung als auch im laufenden Betrieb. Unzuverlässige Mitarbeiter werden von den Tätigkeiten des ZDA ausgeschlossen.

Alle im Betrieb eines ZDA tätigen Personen müssen über die für die Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen. Die Fachkunde wird vor Übernahme einer Aufgabe und über die gesamte Dauer der Tätigkeit durch Schulungen sichergestellt.

Im Falle des Ausscheidens von Mitarbeitern werden ihnen sämtliche Berechtigungen in Bezug auf die ZDA-Tätigkeiten entzogen (zum Beispiel Rechnerzugang, Schlüssel, Unterlagen).

7.4 Prozessbezogene Sicherheitsmaßnahmen

7.4.1 Rollentrennung

Das Prinzip der Rollentrennung sorgt dafür, dass unterschiedliche Rollen (Aufgabenfelder) von verschiedenen Mitarbeitern ausgeübt und verantwortet werden. Im Unterschied zum Vier-Augen-Prinzip müssen die zugehörigen Tätigkeiten nicht zeitgleich erfolgen, sondern können auch asynchron ausgeführt werden.

7.4.2 Rollentrennung im Bereich der administrativen Rollen

Die nach den Sicherheitskonzepten notwendigen Rollentrennungen innerhalb der administrativen Rollen sind bei der Deutschen Rentenversicherung Bund sichergestellt, da die Rollen von Mitarbeitern unterschiedlicher Organisationseinheiten ausgeübt werden. Eine Ausnahme bildet hier nur der Kryptomanager, der in einer Organisationseinheit mit dem Leiter der Zertifizierungsstelle tätig ist.

Die Rolle des Leiters Systemverwaltung darf nicht durch das operative Personal übernommen werden. Es ist nicht zulässig, dass operativ tätiges Personal administrativ in der Systemverwaltung eingesetzt wird.

Dem Leiter Systemverwaltung ist es explizit untersagt, die Rollen

- Systemverwalter Server 1+2 und
- Systemverwalter Netzwerk 1+2

zu übernehmen.

Für die Systemverwalter gelten folgende Rollentrennungen:

- Auf alle Komponenten darf nur im Vier-Augen-Prinzip zugegriffen werden können, das heißt die Rollen Systemverwalter 1 und Systemverwalter 2 derselben technischen Komponente dürfen nicht von einer Person übernommen werden. Diese Rollen werden voneinander getrennt.
- Ein Systemverwalter darf mehrere Komponenten administrieren (vorausgesetzt, er wird nicht gleichzeitig Systemverwalter 1 und 2 derselben technischen Komponente).

7.4.3 Vertretungsregelung

Für besondere Situationen (Urlaubszeit, Krankheit) gibt es für alle Rollen Vertretungsregelungen unter Berücksichtigung der jeweiligen Rollentrennung.

7.4.4 Rufbereitschaft

Es ist sichergestellt, dass der Leiter der Wurzelzertifizierungsstelle und mindestens zwei Personen der Systemverwalter-Gruppe für den Notfall verfügbar sind. Die Erreichbarkeit ist durch Bereitschafts-Mobiltelefone gewährleistet.

7.5 Technische Sicherheitsmaßnahmen

Durch die technischen Sicherheitsmaßnahmen wird der SigG-konforme Betrieb der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung gewährleistet.

An die Verfügbarkeit bestimmter Komponenten, die zur Prüfung der Gültigkeit von Signaturen und zum Sperren von Chipkarten dienen, werden besonders hohe Anforderungen gestellt. Diese IT-Systeme sind deshalb redundant ausgelegt. Außerdem gibt es ein Backup-System für Notfälle. So wird eine Verfügbarkeit von 99,5 % pro Jahr für diese IT-Systeme sichergestellt.

Das Netzwerk als die den zentralen Zertifizierungsdiensten zugrunde liegende Infrastruktur verfügt über ein hohes Sicherheitsniveau. Innerhalb einzelner, physikalisch voneinander

getrennter Sicherheitszonen kontrollieren Firewalls die zulässigen Datenströme bzw. sichern die Übergänge zu externen Netzen ab.

Die Datensicherung gewährleistet, dass Zertifizierungsdienste kurzfristig wieder verfügbar gemacht werden können, wenn ihre Daten verloren gegangen sind. Die Daten müssen vor unbefugtem Zugriff bei der Erstellung, beim Transport und bei der Verwahrung vor Manipulation geschützt werden.

7.6 Dokumentation

Um der Nachvollziehbarkeit bzw. Revisionssicherheit Genüge zu leisten, unterliegt der Zertifizierungsdiensteanbieter einer in SigG und SigV geregelten Dokumentations- und Aufbewahrungspflicht („Archivierung“), das heißt SigG und SigV verpflichten den ZDA, die beim Betrieb anfallenden Dokumentationen für einen bestimmten Zeitraum aufzubewahren. Bei der Deutschen Rentenversicherung Bund folgt die Archivierung von Dokumenten in Papierform der vom SigG für einen akkreditierten ZDA vorgeschriebenen Archivierung.

Die zu einem Zertifikat gehörige Papierdokumentation muss demzufolge 30 Jahre nach Erlöschen der Gültigkeit des Zertifikats aufgehoben werden. Da nach SigG ein qualifiziertes Zertifikat maximal fünf Jahre Gültigkeit besitzen darf, wird die zu einem Zertifikat gehörige Papierdokumentation nach dessen Freischaltung 35 Jahre lang aufbewahrt.

Sowohl Dokumente in Papierform als auch Dokumente in elektronischer Form sind entsprechend zu archivieren. Der Pflicht zur sicheren Aufbewahrung elektronischer Daten wird durch entsprechende Datensicherung der anfallenden elektronischen Dokumente über den vorgeschriebenen Zeitraum nachgekommen.

Die Papierdokumente werden im Archivraum unter Verschluss - in Ordner sortiert - aufbewahrt. Zum Archivraum haben nur der Mitarbeiter Archivierung und der Leiter der Zertifizierungsstellen Zugang. Die Ordner sind vom Mitarbeiter Archivierung dokumenten- bzw. prozessspezifisch anzulegen.

Bei den zu archivierenden Papierdokumenten handelt es sich im Wesentlichen um folgende Dokumente:

1. übergreifende Dokumente, wie beispielsweise das Sicherheitskonzept, Unterlagen zur Fachkunde der im Betrieb tätigen Personen oder die Betriebsanzeige bei der Bundesnetzagentur,
2. die Dokumentation der Key-Ceremony,
3. alle Dokumentationen sicherheitsrelevanter Ereignisse.

7.7 Melden sicherheitsrelevanter Vorfälle

Werden bei den Prozessen sicherheitsrelevante Vorfälle festgestellt, so ist der Leiter der Zertifizierungsstelle unverzüglich einzuschalten. Dieser veranlasst die Untersuchung des sicherheitsrelevanten Vorfalls und gegebenenfalls die Sperrung des Zertifikats.

8 Weitere geschäftliche und rechtliche Regelungen

8.1 Abschluss einer Verwaltungsvereinbarung

Die Deutsche Rentenversicherung Bund als Träger der Wurzelzertifizierungsstelle der Deutschen Rentenversicherung schließt mit dem jeweiligen RV-Träger eine Verwaltungsvereinbarung ab, die die Übernahme der zentralen Dienste eines ZDA regelt.

Die Nutzung des Zeitstempeldienstes wird ebenfalls in einer Verwaltungsvereinbarung geregelt.

8.2 Vertraulichkeit personenbezogener Informationen

Die Wurzelzertifizierungsstelle der Deutschen Rentenversicherung hält die gesetzlichen Bestimmungen zum Schutz der erhobenen personenbezogenen Daten ein (§ 14 SigG, ergänzend BDSG). Der Umfang erhobener personenbezogener Daten von Zertifikatsinhabern richtet sich an der Erforderlichkeit gemäß SigG und SigV aus.

8.3 Haftung des Zertifizierungsdiensteanbieters

Die Wurzelzertifizierungsstelle der Deutschen Rentenversicherung haftet nach den Bestimmungen der jeweiligen Verwaltungsvereinbarung sowie nach den allgemeinen gesetzlichen Vorgaben. Für die qualifizierten Signaturzertifikate gelten die Haftungsregelungen des SigG.

8.4 Pflichten der Zertifikatsinhaber

Die Pflichten der Zertifikatsinhaber richten sich nach den Bestimmungen des Signaturgesetzes und den (Verwaltungs-)Vereinbarungen.

8.5 Gültigkeit dieses Dokumentes

8.5.1 Gültigkeitszeitraum

Dieses Dokument ist vom Tage seiner Veröffentlichung an gültig. Seine Gültigkeit endet nur mit der Einstellung der Zertifizierungsdienste.

8.5.2 Vorzeitiger Ablauf der Gültigkeit

Die Gültigkeit dieses Dokumentes endet vorzeitig mit der Veröffentlichung einer neuen Version.

8.6 Änderungen / Ergänzungen dieses Dokumentes

8.6.1 Verfahren für die Änderung / Ergänzung dieses Dokumentes

Die Deutsche Rentenversicherung Bund behält sich die Änderung dieses Dokuments vor. Diese kann insbesondere durch eine Weiterentwicklung der technischen oder rechtlichen Gegebenheiten erforderlich sein.

8.6.2 Benachrichtigungsverfahren und Veröffentlichungsperioden

Sollten die Änderungen sicherheitsrelevante Aspekte oder die Verfahren hinsichtlich der Zertifikatsinhaber betreffen, wie beispielsweise Änderungen des Registrierungsablaufs, des Verzeichnis- und Sperrdiensts, der Kontaktinformationen oder der Haftung, wird der Zertifizierungsdiensteanbieter die Zertifikatsinhaber in geeigneter Weise benachrichtigen.

Hinsichtlich übriger Änderungen, insbesondere der Verbesserung geringfügiger redaktioneller Versehen oder der Beifügung von Erläuterungen, kann eine Benachrichtigung der Zertifikatsinhaber unterbleiben.

8.6.3 Änderungsbedingungen

Bei Ergänzungen oder Modifikationen der CPS entscheidet die Zertifizierungsstelle, ob sich daraus signifikante Änderungen der Sicherheit der Zertifizierungsdienste, des Vertrauens, welches den Zertifikaten entgegengebracht werden kann, der Rechte und Pflichten der Teilnehmer oder der Anwendbarkeit der Zertifikate ergeben. Falls dies der Fall ist, wird die Versionsnummer auf die nächste volle Nummer erhöht.

8.6.4 Schriftlichkeitsgebot

Die jeweils aktuelle Schriftversion dieses Textes ersetzt sämtliche vorhergehende Versionen. Mündliche Kundmachungen erfolgen nicht.

9 Zertifikatsprofile

In den Zertifikatsprofilen werden in den Namen so genannte Platzhalter verwendet, um die Definition generisch zu halten. Die verwendeten dynamischen Platzhalter ergeben sich aus Tabelle 3:

Tabelle 3: Dynamische Platzhalter

Pos	Platzhalter	Beschreibung
1	<RV-Träger>	Name des RV-Trägers
2	<RVTNR>	Nummer des RV-Trägers
3	<CERTSN>	Zertifikats-Seriennummer

Die Profile für OCSP-Signer-Zertifikate der Mitarbeiter-CAs sind in den Certification Practice Statements der Mitarbeiter-CAs der jeweiligen ZDA der Deutschen Rentenversicherung beschrieben.

Die Profile für die CA-Zertifikate der NQ DRV Server CA und der NQ 70 Server CA sind in den jeweiligen Certificate Policies und Certification Practice Statements der Deutschen Rentenversicherung Bund beschrieben. Der Betrieb dieser Server-CAs wird mit dem Auslaufen von deren CA-Zertifikaten am 28.07.2011 eingestellt.

Die Profile für OCSP-Signer-Zertifikate der Server-CAs sind in den jeweiligen Certificate Policies und Certification Practice Statements der Deutschen Rentenversicherung Bund beschrieben.

9.1 Zertifikate der Wurzel-CAs

9.1.1 Zertifikat der QC Root CA

Pos	Bezeichnung	Kritisch	Inhalt	Wert
1	Version		Zertifikatsformat	2
2	SerialNumber		Seriennummer des Zertifikates	Automatisch durch CM
3	Signature		ID des verwendeten Algorithmus	sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11)
4	Issuer		DN der ausgebenden CA	OU=“QC Root CA“ O=“Deutsche Rentenversicherung“ C=“DE“
5	Validity		Gültigkeitszeitraum des Zertifikates	5 Jahre ab Ausgabedatum
6	Subject		DN des Zertifikatsinhabers	OU=“QC Root CA“ O=“Deutsche Rentenversicherung“ C=“DE“
7	SubjectPublicKey		Public Key, der beglaubigt werden soll	Schlüssellänge: 2048 Bit Schlüsselspeicher: CardOS V4.3B Chipkarte
8	SubjectKeyIdentifier	Nein	Hash des öffentlichen Schlüssels im Zertifikat	Automatisch durch CM
9	KeyUsage	Ja	Verwendungszweck des Schlüssels	KeyCertSign (RFC 3280)
10	CertificatePolicies	Nein	OID der “Certificate Policy” und die URL, unter der die Policy mit einem Browser abgerufen werden kann	OID= 1.3.6.1.4.1.22204.1.8.1.1.1 URL=“http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html”
11	BasicConstraints	Ja	Einschränkungen des Zertifikates	CA=True
12	QCStatement	Nein	Das QCStatement ‚QCCompliance’ bestätigt, dass die Policy der CA der EU-Signaturrichtlinie entspricht.	
13	SubjectDirectoryAttributes	Nein	Leiter der Wurzelzertifizierungsstelle der Rentenversicherung, x ist eine fortlaufende Nummer ab 1	CN=“QC Wurzelzertifizierungsstelle Deutsche Rentenversicherung x:PN“

9.1.2 Zertifikat der NQ Root CA

Pos	Bezeichnung	Kritisch	Inhalt	Wert
1	Version		Zertifikatsformat	2
2	SerialNumber		Seriennummer des Zertifikates	Automatisch durch CM
3	Signature		ID des verwendeten Algorithmus	sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11)
4	Issuer		DN der ausgebenden CA	OU=“NQ Root CA“ O=“Deutsche Rentenversicherung“ C=“DE“
5	Validity		Gültigkeitszeitraum des Zertifikates	5 Jahre ab Ausgabedatum
6	Subject		DN des Zertifikatsinhabers	OU=“NQ Root CA“ O=“Deutsche Rentenversicherung“ C=“DE“
7	SubjectPublicKey		Public Key, der beglaubigt werden soll	Schlüssellänge: 2048 Bit Schlüsselspeicher: HSM
8	SubjectKeyIdentifier	Nein	Hash des öffentlichen Schlüssels im Zertifikat	Automatisch durch CM
9	KeyUsage	Ja	Verwendungszweck des Schlüssels	keyCertSign (RFC 3280) crlSign (RFC 3280)
10	CertificatePolicies	Nein	OID der “Certificate Policy” und die URL, unter der die Policy mit einem Browser abgerufen werden kann	OID= 1.3.6.1.4.1.22204.1.8.2.1.1 URL=”http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html”
11	BasicConstraints	Ja	Einschränkungen des Zertifikates	CA=True

9.2 CRL-Signer-Zertifikate

9.2.1 CRL-Signer-Zertifikat der QC Root CA

Seit dem 23.01.2009 wird kein CRL-Signer-Zertifikat der "QC Root CA" mehr verwendet, weil ab diesem Zeitpunkt bis auf Weiteres keine Sperrlisten (CRLs und Delta-CRLs) für die "QC Root CA" mehr bereitgestellt werden.

Pos	Bezeichnung	Kritisch	Inhalt	Wert
1	Version		Zertifikatsformat	2
2	SerialNumber		Seriennummer des Zertifikates	Automatisch durch CM
3	Signature		ID des verwendeten Algorithmus	sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11)
4	Issuer		DN der ausgebenden CA	OU=“QC Root CA“ O=“Deutsche Rentenversicherung“ C=“DE“
5	Validity		Gültigkeitszeitraum des Zertifikates	Maximal 5 Jahre ab Ausgabedatum, nicht länger gültig als das Zertifikat der QC Root CA
6	Subject		DN des Zertifikatsinhabers	OU=“QC Root CA“ O=“Deutsche Rentenversicherung“ C=“DE“
7	SubjectPublicKey		Public Key, der beglaubigt werden soll	Schlüssellänge: 2048 Bit Schlüsselspeicher: HSM
8	SubjectKeyIdentifier	Nein	Hash des öffentlichen Schlüssels im Zertifikat	Automatisch durch CM
9	AuthorityKeyIdentifier	Nein	KeyIdentifier der ausstellenden CA	Automatisch durch CM
10	KeyUsage	Ja	Verwendungszweck des Schlüssels	crlSign (RFC 3280)
11	CertificatePolicies	Nein	OID der “Certificate Policy” und die URL, unter der die Policy mit einem Browser abgerufen werden kann	OID=1.3.6.1.4.1.22204.1.8.1.1.1 URL=”http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html”
12	BasicConstraints	Ja	Einschränkungen des Zertifikates	CA=True

Pos	Bezeichnung	Kritisch	Inhalt	Wert
13	IssuerAltNames	Nein	Eine LDAP-URL und eine HTTP-URL, unter der das CA-Zertifikat der ausstellenden CA abgerufen werden kann	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ cn=<CERTSN>, ou=QC%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=cACertificate“ URL2 =“http://dir.tc.deutsche- rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.cer?dn= cn%3D<CERTSN>%2C ou%3DQC%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=cACertificate“

9.3 OCSP-Signer-Zertifikate und TSP-Signer-Zertifikate der Wurzel-CAs

9.3.1 OCSP-Signer-Zertifikat der QC Root CA

Pos	Bezeichnung	Kritisch	Inhalt	Wert
1	Version		Zertifikatsformat	2
2	SerialNumber		Seriennummer des Zertifikates	Automatisch durch CM
3	Signature		ID des verwendeten Algorithmus	sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11)
4	Issuer		DN der ausgebenden CA	OU=“QC Root CA“ O=“Deutsche Rentenversicherung“ C=“DE“
5	Validity		Gültigkeitszeitraum des Zertifikates	Maximal 5 Jahre ab Ausgabedatum, nicht länger gültig als das Zertifikat der QC Root CA
6	Subject		DN des Zertifikatsinhabers	CN=“QC Root OCSP“ OU=“QC Root CA“ O=“Deutsche Rentenversicherung“ C=“DE“
7	SubjectPublicKey		Public Key, der beglaubigt werden soll	Schlüssellänge: 2048 Bit Schlüsselspeicher: CardOS V4.3B Chipkarte
8	AuthorityKeyIdentifier	Nein	KeyIdentifier der ausstellenden CA	Automatisch durch CM
9	KeyUsage	Ja	Verwendungszweck des Schlüssels	nonRepudiation (RFC 3280)
10	ExtendedKeyUsage	Ja	Erweiterter Verwendungszweck des Schlüssels	OCSPSigning (RFC 3280) (OID = 1.3.6.1.5.5.7.3.9)
11	CertificatePolicies	Nein	OID der “Certificate Policy” und die URL, unter der die Policy mit einem Browser abgerufen werden kann	OID= 1.3.6.1.4.1.22204.1.8.1.1.1 URL=”http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html”
12	BasicConstraints	Ja	Einschränkungen des Zertifikates	CA=False

Pos	Bezeichnung	Kritisch	Inhalt	Wert
13	IssuerAltNames	Nein	Eine LDAP-URL und eine HTTP-URL, unter der das CA-Zertifikat der ausstellenden CA abgerufen werden kann	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ cn=<CERTSN>, ou=QC%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=cACertificate“ URL2 =“http:// dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.cer?dn= cn%3D<CERTSN>%2C ou%3DQC%20Root%20CA%2C cn%3Dpublic%2C o%3DDRV%2C c%3DDE& attrname=cACertificate“
14	QCStatements	Nein	Das QCStatement ‚QCCompliance’ bestätigt, dass die Policy der CA der EU-Signaturrichtlinie entspricht.	
15	SubjectDirectoryAttributes	Nein	Systemverwalter OCSP 1, x ist eine fortlaufende Nummer ab 1	CN=“QC OCSP Deutsche Rentenversicherung x:PN“

Pos	Bezeichnung	Kritisch	Inhalt	Wert
16	CRLDistributionPoints seit 23.01.2009: – keine Sperrlisten – Parameter in neuen Zertifikaten nicht enthalten	Nein	Eine LDAP-URL und eine HTTP-URL, unter der die Sperrliste (CRL) der QC Root CA abgerufen werden kann Seit dem 23.01.2009 werden bis auf Weiteres keine Sperrlisten (CRLs und Delta-CRLs) der "QC Root CA" mehr bereitgestellt. Ab dem Schlüsselwechsel Mitte 2009 werden OCSP-Signer-Zertifikate der "QC Root CA" so ausgestellt, dass sie keinen Parameter CRLDistributionPoints enthalten.	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ ou=QC%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=certificateRevocationList“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.crl?dn= ou%3DQC%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=certificateRevocationList“

9.3.2 OCSP-Signer-Zertifikat der NQ Root CA

Pos	Bezeichnung	Kritisch	Inhalt	Wert
1	Version		Zertifikatsformat	2
2	SerialNumber		Seriennummer des Zertifikates	Automatisch durch CM
3	Signature		ID des verwendeten Algorithmus	sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11)
4	Issuer		DN der ausgebenden CA	OU=“NQ Root CA“ O=“Deutsche Rentenversicherung“ C=“DE“
5	Validity		Gültigkeitszeitraum des Zertifikates	Maximal 5 Jahre ab Ausgabedatum, nicht länger gültig als das Zertifikat der NQ Root CA
6	Subject		DN des Zertifikatsinhabers	CN=“NQ Root OCSP“ OU=“NQ Root CA“ O=“Deutsche Rentenversicherung“ C=“DE“
7	SubjectPublicKey		Public Key, der beglaubigt werden soll	Schlüssellänge: 2048 Bit Schlüsselspeicher: HSM
8	AuthorityKeyIdentifier	Nein	KeyIdentifier der ausstellenden CA	Automatisch durch CM
9	KeyUsage	Ja	Verwendungszweck des Schlüssels	nonRepudiation (RFC 3280)
10	ExtendedKeyUsage	Ja	Erweiterter Verwendungszweck des Schlüssels	OCSPSigning (RFC 3280) (OID = 1.3.6.1.5.5.7.3.9)
11	CertificatePolicies	Nein	OID der “Certificate Policy” und die URL, unter der die Policy mit einem Browser abgerufen werden kann	OID= 1.3.6.1.4.1.22204.1.8.2.1.1 URL=”http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html”
12	BasicConstraints	Ja	Einschränkungen des Zertifikates	CA=False

Pos	Bezeichnung	Kritisch	Inhalt	Wert
13	IssuerAltNames	Nein	Eine LDAP-URL und eine HTTP-URL, unter der das CA-Zertifikat der ausstellenden CA abgerufen werden kann.	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ cn=<CERTSN>, ou=NQ%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=cACertificate“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.cer?dn= cn%3D<CERTSN>%2C ou%3DNQ%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=cACertificate“
14	CRLDistributionPoints	Nein	Eine LDAP-URL und eine HTTP-URL, unter der die Sperrliste (CRL) der NQ Root CA abgerufen werden kann	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ ou=NQ%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=certificateRevocationList“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.crl?dn= ou%3DNQ%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=certificateRevocationList“

9.3.3 TSP-Signer-Zertifikat der QC Root CA

Pos	Bezeichnung	Kritisch	Inhalt	Wert
1	Version		Zertifikatsformat	2
2	SerialNumber		Seriennummer des Zertifikates	Automatisch durch CM
3	Signature		ID des verwendeten Algorithmus	sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11)
4	Issuer		DN der ausgebenden CA	OU="QC Root CA" O="Deutsche Rentenversicherung" C="DE"
5	Validity		Gültigkeitszeitraum des Zertifikates	Maximal 5 Jahre ab Ausgabedatum, nicht länger gültig als das Zertifikat der QC Root CA
6	Subject		DN des Zertifikatsinhabers	CN="QC Root TSP" OU="QC Root CA" O="Deutsche Rentenversicherung" C="DE"
7	SubjectPublicKey		Public Key, der beglaubigt werden soll	Schlüssellänge: 2048 Bit Schlüsselspeicher: CardOS V4.3B Chipkarte
8	AuthorityKeyIdentifier	Nein	KeyIdentifier der ausstellenden CA	Automatisch durch CM
9	KeyUsage	Ja	Verwendungszweck des Schlüssels	nonRepudiation (RFC 3280)
10	ExtendedKeyUsage	Ja	Erweiterter Verwendungszweck des Schlüssels	timeStamping (RFC 3280) (OID = 1.3.6.1.5.5.7.3.8)
11	CertificatePolicies	Nein	OID der "Certificate Policy" und die URL, unter der die Policy mit einem Browser abgerufen werden kann	OID= 1.3.6.1.4.1.22204.1.8.1.1.3 URL="http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html"
12	BasicConstraints	Ja	Einschränkungen des Zertifikates	CA=False

Pos	Bezeichnung	Kritisch	Inhalt	Wert
13	IssuerAltNames	Nein	Eine LDAP-URL und eine HTTP-URL, unter der das CA-Zertifikat der ausstellenden CA abgerufen werden kann	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ cn=<CERTSN>, ou=QC%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=cACertificate“ URL2 =”http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.cer?dn= cn%3D<CERTSN>%2C ou%3DQC%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=cACertificate”
14	QCStatements	Nein	Das QCStatement ‚QCCompliance’ bestätigt, dass die Policy der CA der EU-Signaturrichtlinie entspricht.	
15	SubjectDirectoryAttributes	Nein	Systemverwalter TSP 1, x ist eine fortlaufende Nummer ab 1	CN= QC TSP Deutsche Rentenversicherung x:PN

Pos	Bezeichnung	Kritisch	Inhalt	Wert
16	CRLDistributionPoints seit 23.01.2009: – keine Sperrlisten – Parameter in neuen Zertifikaten nicht enthalten	Nein	Eine LDAP-URL und eine HTTP-URL, unter der die Sperrliste (CRL) der QC Root CA abgerufen werden kann Seit dem 23.01.2009 werden bis auf Weiteres keine Sperrlisten (CRLs und Delta-CRLs) der "QC Root CA" mehr bereitgestellt. Ab dem Schlüsselwechsel Mitte 2009 werden TSP-Signer-Zertifikate der "QC Root CA" so ausgestellt, dass sie keinen Parameter CRLDistributionPoints enthalten.	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ ou=QC%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=certificateRevocationList“ URL2 =”http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.crl?dn= ou%3DQC%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=certificateRevocationList”
17	AuthorityInfoAccess	Nein	URL, unter welcher der OCSP-Responder gefunden wird	URL=“http://ocsp-rootqc.tc.deutsche-rentenversicherung.de”

9.4 Zertifikate der Mitarbeiter-CAs

9.4.1 Zertifikat der QC <RVTNR> Mitarbeiter CA

Pos	Bezeichnung	Kritisch	Inhalt	Wert
1	Version		Zertifikatsformat	2
2	SerialNumber		Seriennummer des Zertifikates	Automatisch durch CM
3	Signature		ID des verwendeten Algorithmus	sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11)
4	Issuer		DN der ausgebenden CA	OU="QC Root CA" O="Deutsche Rentenversicherung" C="DE"
5	Validity		Gültigkeitszeitraum des Zertifikates	Maximal 4 Jahre ab Ausgabedatum, nicht länger gültig als das Zertifikat der QC Root CA
6	Subject		DN des Zertifikatsinhabers	OU="QC <RVTNR> Mitarbeiter CA" O=<RV-Träger> C="DE"
7	SubjectPublicKey		Public Key, der beglaubigt werden soll	Schlüssellänge: 2048 Bit Schlüsselspeicher: CardOS V4.3B Chipkarte
8	SubjectKeyIdentifier	Nein	Hash des öffentlichen Schlüssels im Zertifikat	Automatisch durch CM
9	KeyUsage	Ja	Verwendungszweck des Schlüssels	keyCertSign (RFC 3280)
10	CertificatePolicies	Nein	OID der "Certificate Policy" und die URL, unter der die Policy mit einem Browser abgerufen werden kann	OID=1.3.6.1.4.1.22204.1.8.1.1.1 URL="http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html"
11	BasicConstraints	Ja	Einschränkungen des Zertifikates	CA=True
12	AuthorityKeyIdentifier	Nein	KeyIdentifier der ausstellenden CA	Automatisch durch CM

Pos	Bezeichnung	Kritisch	Inhalt	Wert
13	CRLDistributionPoints seit 23.01.2009: – keine Sperrlisten – Parameter in neuen Zertifikaten nicht enthalten	Nein	Eine LDAP-URL und eine HTTP-URL, unter der die Sperrliste (CRL) der QC Root CA abgerufen werden kann Seit dem 23.01.2009 werden bis auf Weiteres keine Sperrlisten (CRLs und Delta-CRLs) der "QC Root CA" mehr bereitgestellt. Vor dem 23.01.2009 ausgestellte Zertifikate einer „QC <RVTNR> Mitarbeiter CA“ enthalten noch den Parameter CRLDistributionPoints. Zertifikate einer „QC <RVTNR> Mitarbeiter CA“, die nach dem 23.01.2009 ausgestellt werden, enthalten keinen Parameter CRLDistributionPoints.	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ ou=QC%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=certificateRevocationList“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.crl?dn= ou%3DQC%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=certificateRevocationList“
14	AuthorityInfoAccess	Nein	URL, unter welcher der OCSP-Responder für die ausstellende CA gefunden wird	URL=“http://ocsp-rootqc.tc.deutsche-rentenversicherung.de”
15	IssuerAltNames	Nein	Eine LDAP-URL und eine HTTP-URL, unter der das Zertifikat der QC Root CA abgerufen werden kann.	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ cn=<CERTSN>, ou=QC%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=cACertificate“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.cer?dn= cn%3D<CERTSN>%2C ou%3DQC%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=cACertificate“

Pos	Bezeichnung	Kritisch	Inhalt	Wert
16	QCStatement	Nein	Das QCStatement ‚QCCompliance' bestätigt, dass die Policy der CA der EU-Signaturrichtlinie entspricht.	
17	SubjectDirectory Attributes	Nein	Leiter der Wurzelzertifizierungsstelle der Rentenversicherung, x ist eine fortlaufende Nummer ab 1	CN="QC Zertifizierungsstelle <RV-Träger> x:PN"

9.4.2 Zertifikat der NQ <RVTNR> Mitarbeiter CA

Pos	Bezeichnung	Kritisch	Inhalt	Wert
1	Version		Zertifikatsformat	2
2	SerialNumber		Seriennummer des Zertifikates	Automatisch durch CM
3	Signature		ID des verwendeten Algorithmus	sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11)
4	Issuer		DN der ausgebenden CA	OU="NQ Root CA" O="Deutsche Rentenversicherung" C="DE"
5	Validity		Gültigkeitszeitraum des Zertifikates	Maximal 4 Jahre ab Ausgabedatum, nicht länger gültig als das Zertifikat der NQ Root CA
6	Subject		DN des Zertifikatsinhabers	OU="NQ <RVTNR> Mitarbeiter CA" O=<RV-Träger> C="DE"
7	SubjectPublicKey		Public Key, der beglaubigt werden soll	Schlüssellänge: 2048 Bit Schlüsselspeicher: HSM
8	SubjectKeyIdentifier	Nein	Hash des öffentlichen Schlüssels im Zertifikat	Automatisch durch CM
9	KeyUsage	Ja	Verwendungszweck des Schlüssels	keyCertSign (RFC 3280) crlSign (RFC 3280)
10	CertificatePolicies	Nein	OID der "Certificate Policy" und die URL, unter der die Policy mit einem Browser abgerufen werden kann	OID=1.3.6.1.4.1.22204.1.8.2.1.1 URL="http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html"
11	BasicConstraints	Ja	Einschränkungen des Zertifikates	CA=True
12	AuthorityKeyIdentifier	Nein	KeyIdentifier der ausstellenden CA	Automatisch durch CM

Pos	Bezeichnung	Kritisch	Inhalt	Wert
13	CRLDistributionPoints	Nein	Eine LDAP-URL und eine HTTP-URL, unter der die Sperrliste (CRL) der NQ Root CA abgerufen werden kann	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ ou=NQ%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=certificateRevocationList“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.crl?dn= ou%3DNQ%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=certificateRevocationList“
14	AuthorityInfoAccess	Nein	URL, unter welcher der OCSP-Responder für die ausstellende CA gefunden wird	URL=“http://ocsp-root.tc.deutsche-rentenversicherung.de”
15	IssuerAltNames	Nein	Eine LDAP-URL und eine HTTP-URL, unter der das Zertifikat der NQ Root CA abgerufen werden kann	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ cn=<CERTSN>, ou=NQ%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=cACertificate“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.cer?dn= cn%3D<CERTSN>%2C ou%3DNQ%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=cACertificate“

9.5 Zertifikate der Server-CAs

9.5.1 Zertifikat der NQ DRV CA

Pos	Bezeichnung	Kritisch	Inhalt	Wert
1	Version		Zertifikatsformat	2
2	SerialNumber		Seriennummer des Zertifikates	Automatisch durch CM
3	Signature		ID des verwendeten Algorithmus	sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11)
4	Issuer		DN der ausgebenden CA	OU=“NQ Root CA“ O=„Deutsche Rentenversicherung“ C=“DE“
5	Validity		Gültigkeitszeitraum des Zertifikates	Maximal 4 Jahre ab Ausgabedatum, nicht länger gültig als das Zertifikat der NQ Root CA
6	Subject		DN des Zertifikatsinhabers	OU=“NQ DRV CA“ O=„Deutsche Rentenversicherung“ C=“DE“
7	SubjectPublicKey		Public Key, der beglaubigt werden soll	Schlüssellänge: 2048 Bit Schlüsselspeicher: Eracom-HSM des CCM-Servers
8	SubjectKeyIdentifier	Nein	Hash des öffentlichen Schlüssels im Zertifikat	Automatisch durch CM
9	KeyUsage	Ja	Verwendungszweck des Schlüssels	keyCertSign (RFC 3280) crlSign (RFC 3280)
10	CertificatePolicies	Nein	OID der “Certificate Policy” und die URL, unter der die Policy mit einem Browser abgerufen werden kann	OID=1.3.6.1.4.1.22204.1.8.2.1.1 URL=„http://www.deutsche-rentenversicherung-bund.de/“
11	BasicConstraints	Ja	Einschränkungen des Zertifikates	CA=True
12	AuthorityKeyIdentifier	Nein	KeyIdentifier der ausstellenden CA	Automatisch durch CM

13	CRLDistributionPoints	Nein	Eine LDAP-URL und eine HTTP-URL, unter der die Sperrliste (CRL) der NQ Root CA abgerufen werden kann	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ ou=NQ%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=certificateRevocationList“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.crl?dn= ou%3DNQ%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=certificateRevocationList“
14	AuthorityInfoAccess	Nein	URL, unter welcher der OCSP-Responder für die ausstellende CA gefunden wird	URL=“http://ocsp-root.tc.deutsche-rentenversicherung.de”
15	IssuerAltNames	Nein	Eine LDAP-URL und eine HTTP-URL, unter der das Zertifikat der NQ Root CA abgerufen werden kann	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ cn=<CERTSN>, ou=NQ%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=cACertificate“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.cer?dn= cn%3D<CERTSN>%2C ou%3DNQ%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=cACertificate“

9.5.2 Zertifikat der NQ DRV WAN01 CA

Pos	Bezeichnung	Kritisch	Inhalt	Wert
1	Version		Zertifikatsformat	2
2	SerialNumber		Seriennummer des Zertifikates	Automatisch durch CM
3	Signature		ID des verwendeten Algorithmus	sha1withRSAEncryption
4	Issuer		DN der ausgebenden CA	OU=“NQ Root CA“ O=„Deutsche Rentenversicherung“ C=“DE“
5	Validity		Gültigkeitszeitraum des Zertifikates	Maximal 4 Jahre ab Ausgabedatum, nicht länger gültig als das Zertifikat der NQ Root CA
6	Subject		DN des Zertifikatsinhabers	OU=“NQ DRV WAN01 CA“ O=„Deutsche Rentenversicherung“ C=“DE“
7	SubjectPublicKey		Public Key, der beglaubigt werden soll	Schlüssellänge: 2048 Bit Schlüsselspeicher: Eracom-HSM des CCM-Servers
8	SubjectKeyIdentifier	Nein	Hash des öffentlichen Schlüssels im Zertifikat	Automatisch durch CM
9	KeyUsage	Ja	Verwendungszweck des Schlüssels	keyCertSign (RFC 3280) crlSign (RFC 3280)
10	CertificatePolicies	Nein	OID der “Certificate Policy” und die URL, unter der die Policy mit einem Browser abgerufen werden kann	OID=1.3.6.1.4.1.22204.1.8.2.1.1 URL=„http://www.deutsche-rentenversicherung-bund.de/“
11	BasicConstraints	Ja	Einschränkungen des Zertifikates	CA=True
12	AuthorityKeyIdentifier	Nein	KeyIdentifier der ausstellenden CA	Automatisch durch CM

13	CRLDistributionPoints	Nein	Eine LDAP-URL und eine HTTP-URL, unter der die Sperrliste (CRL) der NQ Root CA abgerufen werden kann	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ ou=NQ%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=certificateRevocationList“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.crl?dn= ou%3DNQ%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=certificateRevocationList“
14	AuthorityInfoAccess	Nein	URL, unter welcher der OCSP-Responder für die ausstellende CA gefunden wird	URL=“http://ocsp-root.tc.deutsche-rentenversicherung.de”
15	IssuerAltNames	Nein	Eine LDAP-URL und eine HTTP-URL, unter der das Zertifikat der NQ Root CA abgerufen werden kann	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ cn=<CERTSN>, ou=NQ%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=cACertificate“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.cer?dn= cn%3D<CERTSN>%2C ou%3DNQ%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=cACertificate“

10 CRLs

Der Aufbau der CRLs und Delta-CRLs der fortgeschrittenen CAs unterhalb der NQ Root CA ist in den jeweiligen Certificate Policies und Certification Practice Statements beschrieben.

10.1 CRL der QC Root CA

Seit dem 23.01.2009 werden bis auf Weiteres keine CRLs der "QC Root CA" mehr bereitgestellt.

Bis zum 23.01.2009 wurden CRLs für die "QC Root CA" mit folgendem Profil bereitgestellt:

Pos	Bezeichnung	Inhalt	Wert
1	Version	CRL-Format	1
2	Signature	ID des verwendeten Algorithmus	sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11)
3	Issuer	DN des CRL-Signers der zugeordneten CA	OU=“QC Root CA“ O=„Deutsche Rentenversicherung“ C=“DE“
4	ThisUpdate	Zeitpunkt der CRL Erstellung	Automatisch durch CM
5	NextUpdate	Zeitpunkt der nächsten CRL-Erstellung	Zeitpunkt der CRL-Erstellung + 1 Woche Die Erzeugung der CRL findet 4 Tage nach Ausstellung der letzten CRL statt.
6	RevokedCertificates	Liste der gesperrten Zertifikate	
6a	UserCertificate	KeyIdentifier des gesperrten Zertifikates	Automatisch durch CM
6b	RevocationDate	Datum und Zeit der Zertifikatssperre	Zeitpunkt der Sperrung
7	CRLNumber	Fortlaufende Nummer der Sperrlisten	Automatisch durch CM

Pos	Bezeichnung	Inhalt	Wert
8	IssuerAltNames	Eine LDAP-URL und eine HTTP-URL, unter der das CRL-Signer-Zertifikat der ausstellenden CA abgerufen werden kann	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ cn=<CERTSN>, cn=CRL%20Signer, ou=QC%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=cACertificate“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.cer?dn= cn%3D<CERTSN>%2C cn%3DCRL%20Signer%2C ou%3DQC%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=cACertificate“
9	AuthorityKeyIdentifier	KeyIdentifier des ausstellenden CRL-Signers	Automatisch durch CM
10	FreshestCRL	URL der Delta-CRL	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ ou=QC%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=deltaRevocationList“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.crl?dn= ou%3DQC%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=deltaRevocationList“

10.2 Delta-CRL der QC Root CA

Seit dem 23.01.2009 werden bis auf Weiteres keine Delta-CRLs der "QC Root CA" mehr bereitgestellt.

Bis zum 23.01.2009 wurden Delta-CRLs für die "QC Root CA" mit folgendem Profil bereitgestellt:

Pos	Bezeichnung	Inhalt	Wert
1	Version	CRL-Format	1
2	Signature	ID des verwendeten Algorithmus	sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11)
3	Issuer	DN des CRL-Signers der zugeordneten CA	OU=“QC Root CA“ O=„Deutsche Rentenversicherung“ C=“DE“
4	ThisUpdate	Zeitpunkt der Delta-CRL Erstellung	Automatisch durch CM
5	NextUpdate	Zeitpunkt der nächsten Basis-CRL-Erstellung	Siehe übergeordnete CRL.
6	RevokedCertificates	Liste der gesperrten Zertifikate	
6a	UserCertificate	KeyIdentifier des gesperrten Zertifikates	Automatisch durch CM
6b	RevocationDate	Datum und Zeit der Zertifikatssperre	Zeitpunkt der Sperrung
7	DeltaCRLIndicator	Kennzeichen, dass es sich um eine Delta-CRL handelt	id-ce-DeltaCRLIndicator=True baseCRLNumber=CRLNumber der Basis-CRL
8	CRLNumber	Fortlaufende Nummer der Sperrlisten	Automatisch durch CM

Pos	Bezeichnung	Inhalt	Wert
9	IssuerAltNames	Eine LDAP-URL und eine HTTP-URL, unter der das CRL-Signer-Zertifikat der ausstellenden CA abgerufen werden kann	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ cn=<CERTSN>, cn=CRL%20Signer, ou=QC%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=cACertificate“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.cer?dn= cn%3D<CERTSN>%2C cn%3DCRL%20Signer%2C ou%3DQC%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=cACertificate“
10	AuthorityKeyIdentifier	KeyIdentifier des ausstellenden CRL-Signers	Automatisch durch CM

10.3 CRL der NQ Root CA

Pos	Bezeichnung	Inhalt	Wert
1	Version	CRL-Format, Standard = 2	1
2	Signature	ID des verwendeten Algorithmus	sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11)
3	Issuer	DN der ausstellenden CA	OU=“NQ Root CA“ O=„Deutsche Rentenversicherung“ C=“DE“
4	ThisUpdate	Zeitpunkt der CRL Erstellung	Automatisch durch CM
5	NextUpdate	Zeitpunkt der nächsten CRL-Erstellung	Zeitpunkt der CRL-Erstellung + 1 Woche Die Erzeugung der CRL findet 4 Tage nach Ausstellung der letzten CRL statt.
6	RevokedCertificates	Liste der gesperrten Zertifikate	
6a	UserCertificate	KeyIdentifier des gesperrten Zertifikates	Automatisch durch CM
6b	RevocationDate	Datum und Zeit der Zertifikatssperre	Zeitpunkt der Sperrung
7	CRLNumber	Fortlaufende Nummer der Sperrlisten	Automatisch durch CM

Pos	Bezeichnung	Inhalt	Wert
8	IssuerAltNames	Eine LDAP-URL und eine HTTP-URL, unter der das Zertifikat der die CRL ausstellenden CA abgerufen werden kann	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ cn=<CERTSN>, ou=NQ%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=cACertificate“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.cer?dn= cn%3D<CERTSN>%2C ou%3DNQ%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=cACertificate“
9	AuthorityKeyIdentifier	KeyIdentifier der ausstellenden CA	Automatisch durch CM
10	FreshestCRL	URL der Delta-CRL	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ ou=NQ%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=deltaRevocationList“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.crl?dn= ou%3DNQ%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=deltaRevocationList“

10.4 Delta-CRL der NQ Root CA

Pos	Bezeichnung	Inhalt	Wert
1	Version	CRL-Format, Standard = 2	1
2	Signature	ID des verwendeten Algorithmus	sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11)
3	Issuer	DN der ausstellenden CA	OU=“NQ Root CA“ O=„Deutsche Rentenversicherung“ C=“DE“
4	ThisUpdate	Zeitpunkt der Delta-CRL Erstellung	Automatisch durch CM
5	NextUpdate	Zeitpunkt der nächsten Basis-CRL-Erstellung	Siehe übergeordnete CRL.
6	RevokedCertificates	Liste der gesperrten Zertifikate	
6a	UserCertificate	KeyIdentifier des gesperrten Zertifikates	Automatisch durch CM
6b	RevocationDate	Datum und Zeit der Zertifikatssperre	Zeitpunkt der Sperrung
7	DeltaCRLIndicator	Kennzeichen, dass es sich um eine Delta-CRL handelt	id-ce-DeltaCRLIndicator=True baseCRLNumber=CRLNumber der Basis-CRL
8	CRLNumber	Fortlaufende Nummer der Sperrlisten	Automatisch durch CM

Pos	Bezeichnung	Inhalt	Wert
9	IssuerAltNames	Eine LDAP-URL und eine HTTP-URL, unter der das Zertifikat der die Delta-CRL ausstellenden CA abgerufen werden kann	URL1 =“ldap://dir.tc.deutsche-rentenversicherung.de/ cn=<CERTSN>, ou=NQ%20Root%20CA, cn=Public, o=DRV, c=DE? attrname=cACertificate“ URL2 =“http://dir.tc.deutsche-rentenversicherung.de:8089/ servlet/DirXweb/Ca/x.cer?dn= cn%3D<CERTSN>%2C ou%3DNQ%20Root%20CA%2C cn%3DPublic%2C o%3DDRV%2C c%3DDE& attrname=cACertificate“
10	AuthorityKeyIdentifier	KeyIdentifier der ausstellenden CA	Automatisch durch CM

11 Verzeichnisse

11.1 Tabellenverzeichnis

Tabelle 1: Administrative Rollen und ihre Aufgaben 17
Tabelle 2: Namen der Wurzel-CAs 21
Tabelle 3: Dynamische Platzhalter 28